EVVA
access to security

Xesar

System manual Xesar 3.2

Imprint

Product code: I.X.R3-2.TD.HDB.SEN.LN | 24R1

Version: Xesar 3.2 | 3.2.x
Edition: 06/2024 UK
The original operating manual was written in German.

Publisher
EVVA Sicherheitstechnologie GmbH

Responsible for content
EVVA Sicherheitstechnologie GmbH

This edition shall not longer be valid upon publication of a new system manual.

You can find the latest edition in the EVVA download area:

https://www.evva.com/uk-en/service/downloads/

This manual is based on the state of the art at the time of creation. The content of the manual has been checked for consistency with the described hardware and software. Nevertheless, deviations cannot be excluded. 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.

Table of 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 shall conclude the contract for the use of Xesar on the basis of the EVVA GTC (General Terms and Conditions) and EVVA GTC (General Terms and Conditions) for the software for the product.

You can call up the EVVA General Terms and Conditions and EVVA General Terms and Conditions:

❯ **https://www.evva.com/uk-en/legal-notice/**

Please note that the use of the Xesar locking system may trigger legal obligations, in particular data protection authorisation, reporting and registration obligations (e.g. when setting up an information network system), as well as employee co-determination rights when used in companies. The user shall bear the responsibility for the legally compliant use of the product.

The above information must be observed in accordance with the manufacturer's liability for its products as defined in the Product Liability Act and must be communicated to operators and users. Non-compliance releases EVVA from any liability.

Unauthorised use, repair work or modifications not authorised by EVVA and improper service may lead to malfunctions and must therefore be avoided. Changes not expressly approved by EVVA will result in the loss of liability, warranty and separately agreed guarantee claims.

Keep the system components away from small children and pets. Risk of suffocation due to small parts that can be swallowed.

EVVA provides **architects and consulting institutions** with all the product information they need to comply with their information and instruction obligations 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, where applicable.

Additional information can be found in the Xesar product catalogue:

› **https://www.evva.com/uk-en/xesar**

1.2 EVVA Support

With Xesar, you have a sophisticated and tested locking system at your disposal. If you require additional support, please contact your EVVA partner directly.

You can access the list of certified EVVA Partners here:

› **https://www.evva.com/uk-en/retailer-search/**

Activate the “Electronics Partner” filter option to search specifically for EVVA partners who sell electronic EVVA locking systems and have qualified specialist knowledge.

› **http://support.evva.at/xesar/en/**

General information on Xesar can be found here:

› **https://www.evva.com/uk-en/xesar**

1.3 Explanation of symbols

The following symbols are used in the system manual to support illustration:

Symbol	Meaning
	Attention, risk of material damage in the event of non-compliance with the corresponding safety measures
	Notices and additional information
	Hints and recommendations
	Avoidance of errors or error messages
Option	Options
	Links
	Steps with instructions for action

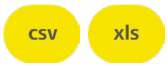
1.4 Explanation of Xesar software symbols

The following symbols are used within the Xesar software, Installation Manager and Periphery Manager:

1.4.1 General

#	Status	Symbol	Explanation
1	Confirm/save		Confirming or saving input
2	Adding		Adding, for example, a new person or installation location
3	Discard entries		Discarding an entry
4	Removal		Removal from e.g. a system, time profile or installation location
5	Edit		Editing a system (Installation Manager)
6	Start application		Starting the system (Installation Manager) or starting the connection between coding station and Xesar software (Xesar Periphery Manager)
7	Stop application		Stopping the system (Installation Manager) or stopping the connection between coding station and Xesar software (Periphery Manager)
8	Download		Download of e.g. Support Information
9	Continue		Continuing to next input
10	Load / transfer		Loading the AdminCard
11	Filter		Display of possible filter settings for the function
12	Update / connect		A task is performed on the dashboard in the backend

#	Status	Symbol	Explanation
13	Not updated / waiting for update / download of update		An update is available and can be downloaded
14	Search		Search for a specific event contribution
15	Maximise		Extending the Field of View
16	Minimise		Reduce the field of view
17	Go to		Open the browser window for the Xesar software
18	System event log		All actions carried out within the Xesar software by users and the system
19	Filtered by areas		Shows all areas to which a person has an access authorisation
20	Filtered by installation locations		Shows all locations to which a person has an access authorisation
21	Filtered by access media		Shows all identification media assigned to a person
22	Filtered by persons		Filter by persons
23	My profile		Edit my user profile: Add description and change personal password
24	Displayed language		Change language
25	Show KeyCredit units		Display of the KeyCredits to be debited (e.g. due to authorisation changes or issuance of new access media)
26	Show Xesar KeyCredit Lifetime		Displayed if KeyCredit Lifetime has been redeemed
27	Event log		Display events, e.g. for a person (all access events relating to a person are filtered and displayed)
28	Help information		Display of help texts

#	Status	Symbol	Explanation
29	Lists export		Export the displayed list as a csv file or as an xls file
30	List view settings		Illustration of list view regarding column selection, number of lines per page, save settings and reset
31	Backup button		A backup of the system data is created in the Installation Manager
32	Logout		End session
33	Battery full		Battery is full
34	Battery warning		Battery is empty, replace batteries as soon as possible
35	Component with cable interface		Access components that can only be synchronised via a cable connection to a tablet
36	Component with wireless BLE interface; BLE is activated		Access components that can be synchronised with wireless BLE and wired to the tablet; BLE function of the access component is activated
37	Component with wireless BLE interface; BLE is disabled		Access components that can be synchronised with wireless BLE and wired to the tablet; BLE function of the component is deactivated
38	Warning		e.g. there are still insecure installation locations

1.4.2 Access media status

#	Status	Visualisation	Explanation
1	Insecure blocked identification medium		The access medium is blocked. There are still insecure installation locations. Take the blacklist using the tablet or an updated access medium to the insecure installation locations.
2	Secure disabled identification medium		The access medium is blocked. There are no insecure installation locations. The system is secure.
3	Unauthorised access medium		The access medium does not have authorisation. Reason e.g. the eligibility period has been exceeded.
4	Currently valid		The access medium is valid and can be used according to the authorisation profile.
5	Currently invalid		The access medium is currently invalid.
6	Current valid access medium becomes an invalid access medium when updated		The access medium is currently valid. It becomes invalid, however, after an update at the online wall reader or at the coding station.
7	A currently invalid access medium reverts to a valid access medium when it is updated		The access medium is currently invalid. However, it will become valid after an update at the online wall reader or at the coding station.
8	Currently invalid access medium, which has a validity interval that lies in the future		The access medium is currently invalid. It remains invalid even after an update at the online wall reader or coding station.
9	Deactivated (blocked) access medium		The access medium has been deactivated; there are no more unsafe installation locations; the calendar is no longer important.

2 Hardware and installation

Check whether the selected Xesar product is suitable for your intended application and follow the instructions in the corresponding data sheet.

› **https://www.evva.com/uk-en/xesar/**

System architecture (sample photo)

2.1 Access components

Xesar has a wide range of components, such as various types of escutcheons, handles, cylinders (including hybrid and cam lock), wall readers and padlocks.

Escutcheon

Handle

Cylinder

Padlock

Wall reader

G2.0 generation access components have a blue or green colour marking under the EVVA logo (plug cover). They only have one plug interface for synchronisation with the tablet.

Generation G2.1 access components can be recognised by the yellow colour marking under the EVVA logo (plug cover).
They feature a wireless and a plug interface for updating using the tablet.
The wireless interface is available as of Xesar version 3.1 and from tablet version Ares BLE 4.2.

If required, the connector interface can also be used to supply emergency power to battery-powered Xesar access components.

As of Xesar version 3.2, generation G2.1 access components can be synchronised and maintained using the Ares BLE 4.2 tablet. In addition to the wired interface, synchronisation can also take place via the BLE wireless interface.
All synchronisation and maintenance tasks, such as configuration changes, event data synchronisation or firmware updates can be performed on all access components within reception range after successful connection.
See also chapter "Carrying out maintenance tasks with a tablet".

DO NOT use pointed objects to open the connector cover!

» Press lightly on the letter E of the EVVA lettering.
» The plug cover at the letter A of the EVVA lettering can be folded forward.

Close the connector cover again after use to protect the connector interface from dust and moisture!

Store batteries in a cool, dry location. Direct 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.

2.1.1 Escutcheon

- Battery-powered access component
- Suitable for use outside and indoors
- Suitable for standard metal frame and solid leaf door locks with handle angle up to 40° with self-locking escape door locks according to EN 179/EN 1125, for fire doors and – in corresponding design – for panic and escape doors with bar handles or push bars according to EN 1125

Observe the provided safety texts, which also contain important information on the installation, use and maintenance of the Xesar access components.

› **https://www.evva.com/uk-en/xesar/**

In outdoor or wet areas, use the appropriate gasket supplied with the product.

When mounting on fire doors, please note that the certificates are only valid with the approvals of the respective door manufacturer.

Escutcheon (sample photo)

1. Visual signalling
2. Reader unit
3. Plug interface (EVVA logo)
   Colour marking (BLE or 3-pin) under the EVVA logo
4. Handle

The reader unit sensor is located on the outside of the escutcheon, between the plug interface and the visual signalling (LED).

The escutcheon signals events both acoustically and visually.
Take note of the list of different acoustic and visual signals in the chapter “Event signalling”.

The escutcheon has a permanent release function. Please refer to the notes on the permanent release function.

Functional principle

The outside handle is disengaged by default – operating the outside handle will not change the position of the latch.

If an authorised identification medium is held in front of the reader unit, the outside handle is mechatronically engaged for 5 seconds. If the outside handle is now pressed, the latch or bolt – depending on the lock type – is drawn.

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

Event log memory

Up to 1,000 events are stored in the event memory. When the event log is full, the entries for the oldest events are overwritten.

Synchronise the events regularly!
This makes it possible to prevent logged events from being overwritten.

Please refer to the data sheet for further specifications.

› **https://www.evva.com/uk-en/xesar/**

Battery replacement

Batteries that are not replaced in time can cause the malfunction of the Xesar escutcheon!

If the batteries are discharged, the escutcheon can only be operated using the emergency power device (optional accessory) and a general master key or fire brigade medium.

If the "Battery low" signal is displayed, the batteries must be replaced immediately. (See also section "Event signalling".) When the "Battery low" signal is displayed for the first time, a maximum of 1,000 openings are possible within a period of 4 weeks. The number of openings depends on the room temperature and may be lower as a result.

Have the batteries changed only by trained specialist personnel!

The battery compartment is located in the upper part of the internal escutcheon plate.
To change the batteries, three batteries (type AAA) and a T8 Torx screwdriver are required.

Always replace all 3 batteries (type AAA) when changing batteries. Please ask your specialist retailer for a list of the recommended battery models.

Do not use rechargeable batteries.

If when changing the battery – the power interruption takes longer than one minute – the Xesar escutcheon must be synchronised using the Xesar tablet!

The procedure for changing batteries in panic door escutcheons is analogous (Only the appearance of the inside escutcheon differs.)

Proceed as follows to change the batteries:

» Loosen the internal escutcheon plate.
Loosen the screw on the underside of the escutcheon with a T8 Torx screwdriver. Turn the Torx screw clockwise until you can release the plate.
» Remove the internal escutcheon plate.
Grasp the internal escutcheon plate by its underside and carefully pull it off the fixing plate. Pull the internal escutcheon plate over the handle. **Make sure that you** do not scratch the handle. (Alternatively, you can remove the inside handle beforehand).
» Replace all batteries. **Make sure** that the batteries are inserted with the correct polarity!

The successful battery change is signalled by "Battery inserted or Reboot of the component"!
Please refer to the chapter "Event signalling".

» Replace the inner plate on the mounting plate.
» Slide the inside plate over the handle.
» Tighten the screw on the underside of the escutcheon with a Torx T8 screwdriver.
» After successful battery replacement, synchronise the component with the tablet and the Xesar software. This transfers the new battery status to the Xesar software.

2.1.2 Handle

- Battery-powered access component
- Suitable for use indoors
- Suitable for solid leaf doors with standard solid leaf door locks with handle angle up to 40°, for escape door locks to EN 179, for fire doors and glass doors in conjunction with corresponding glass-door lock
- Compatible with many European locks because of the compliance with main lock standards and handle angles of up to 40°

Observe the provided safety texts, which also contain important information on the installation, use and maintenance of the Xesar access components.

› **https://www.evva.com/uk-en/xesar/**

When mounting on fire doors, please note that the certificates are only valid with the approvals of the respective door manufacturer.

Handle (sample photo)

1. Visual signalling
2. Reader unit
3. Plug interface (EVVA logo)
   Colour marking (BLE or 3-pin) under the EVVA logo
4. Handle with battery compartment

The reader unit sensor is located on the outside of the handle, between the plug interface and the visual signalling (LED).

The handle signals events both acoustically and visually.

Please note the list of the different acoustic and visual signals in chapter 2.2 Event signalling.

The handle has a permanent release function. Please refer to the notes on the permanent release function.

Functional principle

The outside handle is disengaged by default – operating the outside handle will not change the position of the latch.

If an authorised identification medium is held in front of the reader unit, the outside handle is mechatronically engaged for 5 seconds. If the outside handle is now pressed, the latch or bolt – depending on the lock type – is drawn.

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

Event log memory

Up to 1,000 events are stored in the event memory. When the event log is full, the entries for the oldest events are overwritten.

Synchronise the events regularly!
This makes it possible to prevent logged events from being overwritten.

Please refer to the data sheet for further specifications.

https://www.evva.com/uk-en/xesar/

Battery replacement

Batteries that are not replaced in time can cause the handle to malfunction!

When the batteries are discharged, the handle can only be operated using the emergency power unit (optional accessory) and a master key or fire brigade medium.

If the signal "Battery low" is displayed, the batteries must be replaced immediately. When the "Battery low" signal is displayed for the first time, a maximum of 1,000 openings are possible within a period of 4 weeks. The number of openings depends on the room temperature and can be correspondingly lower.)

Please note the list of the different acoustic and visual signals in chapter 2.2 Event signalling.

Have the batteries changed only by trained specialist personnel!

The battery compartment is located in the outside handle.
To change the battery, you need a battery (type CR123A) and a 2.5 Allen key.

Please ask your specialist retailer for a list of the recommended battery models.

Do not use rechargeable batteries.

When the battery change, i.e the power interruption, lasts longer than one minute, the Xesar handle must be synchronised using the Xesar tablet!

Proceed as follows to change the batteries:

» Remove the outside handle tube.
Using the Allen key, turn the fastening screw clockwise until the handle tube can be removed. **Pay attention** that the fastening screw is only screwed in as far as necessary.
» Replace the batteries. **Make sure** that the battery is inserted with the correct polarity!

The successful battery change is signalled with "Battery inserted or Reboot of the component"!
Note the list of different acoustic and visual signals in the chapter "Event signalling".

» Fit the handle tube back onto the outside handle.
Using the Allen key, unscrew the fixing screw anticlockwise to fix the handle tube. **Pay attention** that the fastening screw is only screwed in as far as necessary.

» After successful battery replacement, synchronise the component with the tablet and the Xesar software. This transfers the new battery status to the Xesar software.

2.1.3 Cylinder

- Battery-powered access component
- Suitable for use outside and indoors
- Suitable for fire protection and escape doors
- Variant already comes with a host of anti-manipulation protection measures.
- The cylinder is available as a half or double cylinder, with electronic release on one or both sides.

Observe the provided safety texts, which also contain important information on the installation, use and maintenance of the Xesar access components.

› **https://www.evva.com/uk-en/xesar/**

When mounting on fire doors, please note that the certificates are only valid with the approvals of the respective door manufacturer.

Cylinder (sample photo)

❶ Visual signalling
❷ Reader unit
❸ Plug interface (EVVA logo)
Colour marking (BLE or 3-pin) under the EVVA logo

The reader unit sensor is located in the cylinder's plastic cap, between the plug interface and the visual signalling (LED).

The cylinder signals events both acoustically and visually.
Take note of the list of different acoustic and visual signals in the chapter "Event signalling".

The cylinder has a permanent release function. Please refer to the notes on the permanent release function.

Functional principle

The electronic outside cylinder thumbturn is disengaged as standard; when the outside thumbturn is operated, the locking cam remains disengaged and the outside thumbturn rotates without taking the locking cam with it.

In the case of cylinders with one-sided electronic release; the mechanical inside always remains engaged and can be operated at any time.

For cylinders with electronic release on both sides, the electronic inside thumbturn acts in the same way as the electronic outside thumbturn.

When an authorised access medium is presented to the reader unit, the outside thumbturn is engaged mechatronically for 5 seconds. The cylinder's cam is carried along when the outside thumbturn is turned.

The door will NOT lock automatically after closing.
The door must be locked manually or by means of a corresponding additional device.

The turning behaviour of the thumbturn may be stiffer due to friction of the seal on the escutcheon or cylinder rosette. There is the option to remove said seals when installing the assembly indoors.

The Xesar cylinder is equipped with a rotation brake as standard. For technical reasons, cylinders with freewheel function (FZG) and anti-panic (FAP) do not have a rotation brake..

Ensure that the rotation brake is installed in the correct position so that no malfunctions occur during operation. Malfunctions in non-approved installation systems are not a production fault and therefore no reason to lodge a complaint.

Event log memory

Up to 1,000 events are stored in the event memory. When the event log is full, the entries for the oldest events are overwritten.

Synchronise the events regularly!
This makes it possible to prevent logged events from being overwritten.

Please refer to the data sheet for further specifications.

› **https://www.evva.com/uk-en/xesar/**

Battery replacement

» Before changing the battery, activate the permanent opening of the cylinder so that it remains engaged.

The cylinder may only be operated with type CR2 batteries.

Please ask your specialist retailer for a list of the recommended battery models.

Do not use rechargeable batteries.

Have the batteries changed only by trained specialist personnel!

If the signal “Battery low” is displayed, the batteries must be replaced immediately. When the “Battery low” signal is displayed for the first time, a maximum of 1,000 openings are possible within a period of 4 weeks. The number of openings depends on the room temperature and can be correspondingly lower.)

If the batteries are discharged, the cylinder can only be operated using the emergency power device (optional accessory) and a general master key or fire service medium.

Replace all batteries in the cylinder when replacing the batteries!

Use the cylinder's special assembly tool for assembling or disassembling the thumb-turn (also when changing the battery).

We recommend that you engage the cylinder using an authorised access medium before removing the batteries. It may be necessary to synchronise the system time via the tablet after replacing batteries.

To replace the cylinders' batteries, proceed as indicated in the installation instructions, but in reverse order.

- Insert the cylinder tool all the way into the recess provided on the rear of the outside thumbturn and screw the tool into the thumbturn (anti-clockwise).
- Remove the cylinder tool and use a Phillips screwdriver (PH1) to unscrew the 3 fastening screws on the rear of the outer thumbturn.
- Remove the thumbturn mounting part.
- Carefully open the locking element in the outside thumbturn by initially moving it carefully before pressing outwards.
- Remove both discharged CR2 batteries and clean the battery contacts using a soft, lint-free cloth.
- Now insert the two new batteries with the correct polarity into the battery compartment and close it again.

When the battery change, i.e the power interruption, lasts longer than one minute, the cylinder must be synchronised with the tablet!

- If the battery change has been carried out correctly, initialisation takes place and the corresponding acoustic signal is emitted. (See chapter “Event signalling”, signal 8 in the signalling table).

- Remount the thumbturn mounting part and fasten it with the 3 fixing screws.

- Insert the cylinder tool all the way into the recess provided on the rear of the outside thumbturn and screw the tool and the thumbturn to the cylinder (in clockwise direction) until you can feel resistance.

- Then turn the cylinder in the opposite direction (anticlockwise) until a “click” is heard.

- Remove the cylinder tool.

- After successful battery replacement, synchronise the component with the tablet and the Xesar software. This transfers the new battery status to the Xesar software.

Fix thumbturn axis

All cylinders in Euro profile design have a service hole on the end face of the electronic module. To facilitate disassembly of the cylinder knob, fix the knob axle with a suitable metallic pin.

The metallic pin must have a minimum diameter of 2 mm and be at minimum length of 40 mm.

To fix the knob axis, proceed as follows:

- Insert a suitable metallic pin – e.g. a 2 mm Allen key – into the service channel on the end face of the Euro profile cylinder.

- When inserting the metal pin, turn the thumbturn about its own axis until the metal pin can be guided significantly deeper into the service channel.

- Hold the metal pin in this position and disassemble the thumbturn as usual using the assembly tool.

- Carefully remove the metal pin after removing the thumbturn.

2.1.4 Hybrid cylinder

- Battery-powered access component
- Suitable for use outside and indoors
- Variant already comes with a host of anti-manipulation protection measures.
- Suitable for fire protection and escape doors.
  For use in escape and panic doors – subject to the mortise lock used – the anti-panic function FAP may be required. For this purpose, observe the corresponding notes or certificates

When mounting on fire doors, please note that the certificates are only valid with the approvals of the respective door manufacturer.

Hybrid cylinder (sample photo)

❶ Visual signalling
❷ Reader unit
❸ Plug interface (EVVA logo)
Colour marking (BLE or 3-pin) under the EVVA logo

The reader unit sensor is located in the cylinder's plastic cap, between the plug interface and the visual signalling (LED).

The cylinder signals events both acoustically and visually.
Take note of the list of different acoustic and visual signals in the chapter "Event signalling".

The cylinder has a permanent release function. Please refer to the notes on the permanent release function.

Functional principle

The hybrid cylinder has a key module on the inside instead of the mechanical thumbturn. This means: Access from the outside is via an electronic authorisation check and access from the inside via a mechanical key.

When the door is closed, it is not automatically locked. The door must be locked manually or by means of a corresponding additional device.

Check whether the selected hybrid cylinder meets your requirements.
Please refer to the data sheet for further specifications.

› **https://www.evva.com/uk-en/service/downloads/**

Hybrid cylinders feature visual and acoustic signals. (See chapter “Event signalling” for explanations of the different signals).

Observe the supplied assembly instructions.

Battery replacement

» Before replacing the battery, activate the permanent opening of the hybrid cylinder so that the hybrid cylinder remains engaged.

The cylinder may only be operated with type CR2 batteries.

Please ask your specialist retailer for a list of the recommended battery models.

Do not use rechargeable batteries.

Have the batteries changed only by trained specialist personnel!

If the signal “Battery low” is displayed, the batteries must be replaced immediately. When the “Battery low” signal is displayed for the first time, a maximum of 1,000 openings are possible within a period of 4 weeks. The number of openings depends on the room temperature and can be correspondingly lower.)

If the batteries are discharged, the hybrid cylinder can only be operated using the emergency power device (optional accessory) and a general master key or fire service medium.

Replace all batteries in the cylinder when replacing the batteries!

Use the cylinder's special assembly tool for assembling or disassembling the thumb-turn (also when changing the battery).

We recommend that you engage the cylinder using an authorised access medium before removing the batteries. It may be necessary to synchronise the system time via the tablet after replacing batteries.

To change the hybrid cylinder's batteries, proceed as indicated in the assembly instructions, but in reverse order.

- Insert the cylinder tool all the way into the recess provided on the rear of the outside thumbturn and screw the tool into the thumbturn (anti-clockwise).
- Remove the cylinder tool and remove the 3 fixing screws with a Phillips screwdriver (PH1) from the rear of the outer thumbturn.
- Remove the thumbturn mounting part.
- Carefully open the locking element in the outside thumbturn by initially moving it carefully before pressing outwards.
- Remove both discharged CR2 batteries and clean the battery contacts using a soft, lint-free cloth.
- Insert the two new batteries with the correct polarity in the battery compartment and close it again.

When the battery change, i.e the power interruption, lasts longer than one minute, the cylinder must be synchronised with the tablet!

- If the battery change has been carried out correctly, initialisation takes place and the corresponding acoustic signal is emitted. (See chapter “Event signalling”, signal 8 in the signalling table).
- Remount the thumbturn mounting part and fasten it with the 3 fixing screws.
- Insert the cylinder tool all the way into the recess provided on the rear of the outside thumbturn and screw the tool and the thumbturn to the cylinder (in clockwise direction) until you can feel resistance.
- Then turn the cylinder in the opposite direction (anticlockwise) until you hear a “click”.
- Remove the cylinder tool.
- After successful battery replacement, synchronise the component with the tablet and the Xesar software. This transfers the new battery status to the Xesar software.

2.1.5 Cam locks

- Battery-powered access component
- Suitable for use outside and indoors
- Suitable for lockers, display cases, various containers and letter boxes.

Cam lock (sample photo)

❶ Visual signalling
❷ Reader unit
❸ Plug interface (EVVA logo)
Colour marking (BLE or 3-pin) under the EVVA logo

The reader unit sensor is located in the cylinder's plastic cap, between the plug interface and the visual signalling (LED).

The cylinder signals events both acoustically and visually.
Take note of the list of different acoustic and visual signals in the chapter "Event signalling".

The cylinder has a permanent release function. Please refer to the notes on the permanent release function.

Functional principle

Access is gained via an electronic authorisation check on the outside of the cam lock.

There is a cam on the inside that serves as a locking mechanism. Locking and unlocking is only possible after a successful authorisation check and by manually turning the cam lock. The electronic thumbturn on the identification side cannot be turned freely without authorisation.

The cam lock is available in different designs and configurations. Check whether the selected cam lock meets your requirements.

Please refer to the data sheet for further specifications.

› **https://www.evva.com/uk-en/service/downloads/**

The cam lock has a visual and an acoustic signal. (See chapter "Event signalling" for explanations of the different signals).

Observe the supplied assembly instructions.

Battery replacement

» Before replacing the battery, activate the permanent opening of the cam lock so that the cam lock remains engaged.

The cylinder may only be operated with type CR2 batteries.

Please ask your specialist retailer for a list of the recommended battery models.

Do not use rechargeable batteries.

Have the batteries changed only by trained specialist personnel!

If the signal "Battery low" is displayed, the batteries must be replaced immediately. When the "Battery low" signal is displayed for the first time, a maximum of 1,000 openings are possible within a period of 4 weeks. The number of openings depends on the room temperature and can be correspondingly lower.)

If the batteries are discharged, the cam lock can only be operated using the emergency power device (optional accessory) and a general master key or fire service medium.

Replace all batteries in the cylinder when replacing the batteries!

Use the cylinder's special assembly tool for assembling or disassembling the thumbturn (also when changing the battery).

We recommend that you engage the cylinder using an authorised access medium before removing the batteries. It may be necessary to synchronise the system time via the tablet after replacing batteries.

To change the batteries of the cam lock, proceed as indicated in the assembly instructions, but in reverse order.

- Insert the cylinder tool all the way into the recess provided on the rear of the outside thumbturn and screw the tool into the thumbturn (anti-clockwise).
- Remove the cylinder tool and open the 3 fastening screws on the rear of the outer thumbturn with a Phillips screwdriver (PH1).
- Remove the thumbturn mounting part.
- Carefully open the lock in the outside thumbturn by initially moving it carefully before pressing outwards.
- Remove both discharged CR2 batteries and clean the battery contacts using a soft, lint-free cloth.
- Insert the two new batteries with the correct polarity into the battery compartment and close it again.

When the battery change, i.e the power interruption, lasts longer than one minute, the cylinder must be synchronised with the tablet!

- If the battery change has been carried out correctly, initialisation takes place and the corresponding acoustic signal is emitted. (See chapter “Event signalling”, signal 8 in the signalling table).
- Remount the thumbturn mounting part and fasten it with the 3 fixing screws.
- Insert the cylinder tool all the way into the recess provided on the rear of the outside thumbturn and screw the tool and the thumbturn to the cylinder (in clockwise direction) until you can feel resistance.
- Then turn the can lock in the opposite direction (anticlockwise) until a “click” is heard.
- Remove the cylinder tool.
- After successful battery replacement, synchronise the component with the tablet and the Xesar software. This transfers the new battery status to the Xesar software.

2.1.6 Padlock

- Battery-powered access component
- Suitable for use outside and indoors
- Suitable for securing of barrier systems, roller blinds, depots and archive containers.
- Can be easily integrated into systems, even at a later date.

Observe the provided safety texts, which also contain important information on the installation, use and maintenance of the Xesar access components.

https://www.evva.com/uk-en/xesar/

Padlock, (sample photo)

1. Visual signalling
2. Reader unit
3. Plug interface (EVVA logo)
   Colour marking (BLE or 3-pin) under the EVVA logo

The reader unit sensor is located in the padlock's plastic cap, between the plug interface and the visual signalling (LED).

The padlock signals events both acoustically and visually.
Take note of the list of different acoustic and visual signals in the chapter “Event signalling”.

The padlock has a permanent release function. Please refer to the notes on the permanent release function.

Functional principle

The padlock's electronic outside thumbturn is disengaged as standard; when the thumbturn is operated, the locking cam remains disengaged and the thumbturn rotates without taking the locking cam with it.

Hold an authorised identification medium to the unit to mechatronically engage the outside thumbturn for five seconds. Both unlocking and locking can only take place after a successful authorisation check. This is done by manually turning electronic thumbturn.
The padlock's locking cam is engaged when the thumbturn is operated.

Event log memory

Up to 1,000 events are stored in the event memory. When the event log is full, the entries for the oldest events are overwritten.

Synchronise the events regularly!
This makes it possible to prevent logged events from being overwritten.

Please refer to the data sheet for further specifications.

https://www.evva.com/uk-en/xesar/

Battery replacement

» Before replacing the battery, activate permanent opening of the padlock so that the padlock remains engaged.

The cylinder may only be operated with type CR2 batteries.

Please ask your specialist retailer for a list of the recommended battery models.

Do not use rechargeable batteries.

Have the batteries changed only by trained specialist personnel!

If the signal “Battery low” is displayed, the batteries must be replaced immediately. When the “Battery low” signal is displayed for the first time, a maximum of 1,000 openings are possible within a period of 4 weeks. The number of openings depends on the room temperature and can be correspondingly lower.)

If the batteries are discharged, the padlock can only be operated using the emergency power device (optional accessory) and a general master key or fire service medium.

Replace all batteries in the cylinder when replacing the batteries!

Use the special installation tool for the padlock to install or remove the thumbturn (also when replacing the battery).

We recommend that you engage the cylinder using an authorised access medium before removing the batteries. It may be necessary to synchronise the system time via the tablet after replacing batteries.

To change the padlock's batteries, proceed as indicated in the installation instructions, but in reverse order.

- Insert the cylinder tool all the way onto the recess provided on the rear of the thumbturn and screw the tool (anti-clockwise) into the thumbturn.
- Remove the cylinder tool and use a Phillips screwdriver (PH1) to unscrew the 3 fastening screws on the rear of the outer thumbturn.
- Remove the thumbturn mounting part.
- Carefully open the locking element in the thumbturn by initially moving it carefully before pressing outwards.
- Remove both discharged CR2 batteries and clean the battery contacts using a soft, lint-free cloth.
- Insert the two new batteries in the correct polarity in the battery compartment and close it again.

When the battery change, i.e the power interruption, lasts longer than one minute, the cylinder must be synchronised with the tablet!

- If the battery change has been carried out correctly, initialisation takes place and the corresponding acoustic signal is emitted. (See chapter “Event signalling”, signal 8 in the signalling table).

- Remount the thumbturn mounting part and fasten it with the 3 fixing screws.
- Insert the cylinder tool all the way into the recess provided on the rear of the outside thumbturn and screw the tool and the thumbturn to the cylinder (in clockwise direction) until you can feel resistance.
- Subsequently turn the cylinder in the opposite direction (anti-clockwise) until a click is heard.
- Remove the cylinder tool.
- After successful battery replacement, synchronise the component with the tablet and the Xesar software. This transfers the new battery status to the Xesar software.

2.1.7 Cylinder tool

The cylinder features a special opening mechanism to protect against manipulation. A special cylinder tool is required for assembly, disassembly and battery replacement.

Cylinder tool (sample photo)

The cylinder tool is not included with the Xesar cylinder.

Option The cylinder tool is optionally available.
Product code: E.ZU.PZ.ZW.V2.

When the battery change, i.e the power interruption, lasts longer than one minute, the cylinder must be synchronised with the tablet!

2.1.8 Wall reader

- For exterior and interior use, flush or surface mounted
- Suitable for safety-relevant areas
- The wall reader is connected to the control unit by means of a connection cable (CAT5 cable, max. 100 m, loop max. = 2 Ohm) and supplied with power via the control unit.
- Electronic locking elements such as motorised cylinders, swing doors or sliding doors can be controlled via the control unit connected to the wall reader.

Observe the provided safety texts, which also contain important information on the installation, use and maintenance of the Xesar access components.

› **https://www.evva.com/uk-en/xesar/**

Use the seal (provided with the product) for outdoor or wet areas and for flush mounting.

Wall reader (sample photo)

1. Visual signalling
2. Reading unit and ON/OFF status light
3. Plug interface (EVVA logo)
   Colour marking (BLE or 3-pin) under the EVVA logo

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

The plug interface serves exclusively for synchronisation with the tablet. The wall reader can NOT be powered by the optional emergency power unit.

The reader unit sensor is located behind the wall reader's glass cover, between the connector interface and the visual signalling (LED). The ON/OFF status light illuminates continuously during operation, making it easier to locate the reading area in a dark environment.

The wall reader signals events both acoustically and visually.
Take note of the list of different acoustic and visual signals in the chapter "Event signalling".

The wall reader has a permanent release function. Please refer to the notes on the permanent release function.

Functional principle

If an access medium is presented to the reader unit, this access medium is checked by the control unit which is connected to the wall reader. If authorised, the respective control unit relay is energised, depending on the jumper position and the configuration. (Note the cover plan, JP2 in the control unit.)

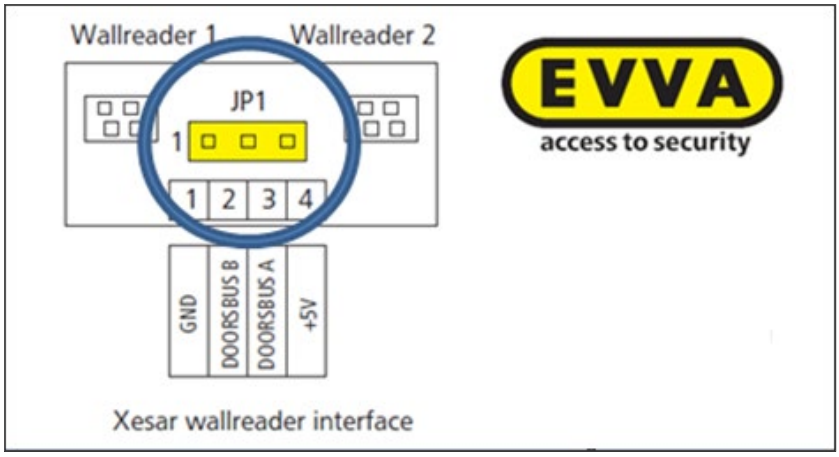
Event log memory

Up to 1,000 events are stored in the control unit's event memory.
When the event memory is full, the oldest event entries are overwritten.

Synchronise the events regularly!
This makes it possible to prevent logged events from being overwritten.

Connection print

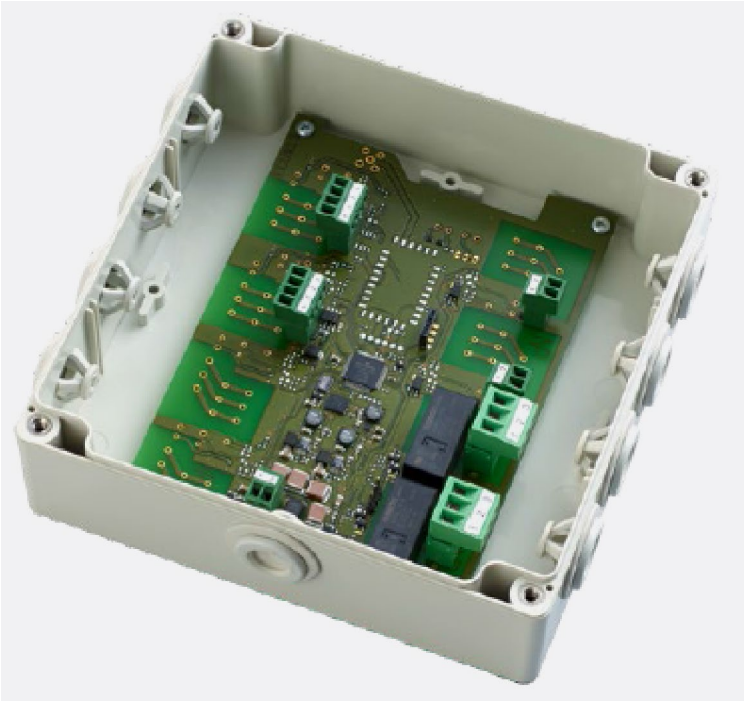
The wall reader is connected to the control unit's connector by means of a connection print.



Connection print for Xesar wall readers (sample photo)

Follow the instructions for jumper setting JP1 in the assembly instructions to avoid a malfunction.

Offline control unit:



Control unit (sample photo)

The wall reader offline control unit can only be operated in conjunction with the wall reader. The maintenance of the offline wall readers is realised using the tablet. Software data is exchanged via tablet, or via XVN with the access media. Up to 2 wall readers can be connected. The control unit connected to the wall reader must be mounted indoors in a manipulation-proof area.

As soon as the control unit has been connected to the power supply for 6 hours the system ensures the time settings are maintained for 72 hours in the event of a power cut.

An external release element (exit button) can be connected to the control unit. When the button is pressed, the door opens and the opening is logged in the event log.

Provided that the control unit has been in operation for at least 6 hours, in the event of a power failure it has a data buffer of max. 72 hours.

Online control unit

The wall reader online control unit can only be operated in conjunction with the wall reader. Each online control unit can be connected to a maximum of 1 wall reader. Control units connected to wall readers must be installed indoors in areas protected from manipulation.

You can find further information on the online wall reader in the chapter “Online wall reader”.

An external release element (exit button) can be connected to the control unit. When the button is pressed, the door opens and the opening is logged in the event log.

For door monitoring, a door contact can be connected to the control unit. The Xesar software logs door opening and closing times and displays the current door status (open/closed).

The online door can be opened remotely and also switched to office mode via the Xesar software.

Online control unit is connected via an Ethernet adapter LAN to the system computer. If the LAN connection is interrupted then the Xesar wall reader behaves like an offline wall reader. The online control unit is supplied with power via the power supply unit. To cope with a power failure, the control unit is equipped with a 72 hour data memory that is fully charged if it has been active for at least 6 hours.

Operate the wall reader control units via an independent power supply and additionally provide a 12 volt uninterruptible power supply. This consequently prevents system failure and safeguards access.

Mains adapter for control unit

The mains adapter for the control unit is optionally available.

Option A power supply unit is optionally available for the control unit: Product code: E.ZU.WL.NT.V2.

2.2 Assembly of access components

Installation of the access components should only be carried out by trained personnel.

Make sure that you follow the described sequence of installation steps to avoid malfunction.

Observe the provided safety texts, which also contain important information on the installation, use and maintenance of the Xesar access components.

❯ **https://www.evva.com/uk-en/xesar/**

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

To support the installation of the access components, EVVA provides, for example, the following tools:

- Language-neutral installation instructions
  The language-neutral installation instructions are enclosed with the corresponding system component. In addition, these are offered on the homepage in the download area.

  ❯ **https://www.evva.com/uk-en/xesar/**

- Product-dependent assembly videos
  Special videos with demonstrations are available showing more complex assembly steps.

  ❯ **http://video.evva.com/tutorials/xesar/**

- Language-neutral drilling template
  The language-neutral drilling template is included with the system component that requires one or more drill holes. In addition, it is offered on the homepage in the download area.

  ❯ **https://www.evva.com/uk-en/xesar/**

A metal drilling template is optionally available for the assembly escutcheons and handles.

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

Option High quality drilling template made of metal:
Product code: E.ZU.BE.BS.V1

2.3 Event signalling

Signal number	Event	Visual signal*	Acoustic signal**	Note
Signal 1	Unlocking attempt with authorised medium	●●●●●	mmmmm	If several cards are in use, signalling only takes place after the last card has been read (Yes / No / no EVVA card present)
Signal 2	End of release	●●●●●	ttttt	
Signal 3	Rejected medium	●●-●●-●●-●●	hh-hh-hh-hh	
Signal 4	Attempt to open with authorised medium when office mode is activated (permanent release)	●●●●--●●●●	tttt--hhhh	
Signal 5	Office mode (permanent release) start	●●●●--●●●●	tttt--hhhh	
Signal 6	Office mode (permanent release) end	●●●●--●●●●	hhhh--tttt	
Signal 7	Opening attempt with authorised medium, signal indicates discharged battery	●●--●●--●●--	h----h----h--- -h----	
Signal 8	Battery inserted or component reboot	●●--●●--●●	tt—mm—hh	Battery charge level indicator; displayed after battery change if necessary
Signal 9	Medium without EVVA segmentation; medium faulty, other system			No signals
Signal 10	Hardware fault	●---●---●---●	mmm---mmm---	
Signal 12	Communication successful	●●●●●	hhhhh	
Signal 13	Communication unsuccessful	●●●●●	ttttt	
Signal 14	Medium authorised offline	●●-●●-●●	mm-mm-mm	
Signal 15	Rejected medium offline	●●-●●-●●	mm-mm-mm	
Signal 16	Online operation failed	●●-●●-●●		

Signal number	Event	Visual signal*	Acoustic signal**	Note
Signalling for G2.1 components:				
Signal 17	Activate BLE (medium 2× stop)	1.: 🟡🟡 2.: 🟡🟡--🔵🔵🔵🔵--🟢🟢🟢🟢	tttt--hhhh	BLE On
Signal 18	Deactivate BLE (medium 2× stop)	1.: 🟡🟡 2.: 🟡🟡--🔵🔵🔵🔵--🔴🔴🔴🔴	hhhh--tttt	BLE Off
Signal 19	Identify BLE component	🟡🟡---🟢🟢---🟢🟢--🟡🟡---🟡🟡---🟢🟢---🟢🟢---🟡🟡	hh---mm---mm---hh---hh---mm---mm---hh	triggered on tablet

* Visual signals (LED): 🟡 = Red 🔴 and Green 🟢 at the same time
** Acoustic signals: h = high-pitched, m = medium-pitched, t = low-pitched.
Each signal corresponds to a duration of 50 ms.
Pauses are indicated by "-".

2.4 Coding station

The coding station is a read/write device for any type of contactless identification media as well as for the contact-based Admin Card, which is one of the system cards (see chapter AdminCard).

The mini coding station cannot be used to operate the AdminCard.

A separate card slot is available for the AdminCard at the front end of the coding station.

» Connect the coding station to the USB port of your computer.

If your operating system does not recognise the coding station automatically,
» install the appropriate driver.

Coding station and mini-coding station (sample photos)

The coding station driver can be downloaded.

› **https://www.hidglobal.com/drivers**

Please refer to the data sheet for further specifications.

2.5 Tablet

The tablet serves to synchronise and transfer information between the Xesar software and the access components.

Tablet (sample photo)

Fully charge your Xesar tablet prior to first use!

The tablet is supplied with the manufacturer's proprietary instruction manual. It is found enclosed within the product packaging.

Do not install additional applications as otherwise EVVA will be unable to safeguard the product security and functionality!

Do not install operating system updates!

As of Xesar version 3.1, generation G2.1 access components can be synchronised and maintained using the Ares BLE 4.2 tablet; in addition to the wired interface synchronisation can also take place via the BLE wireless interface.
For this purpose, the BLE function must be activated on the tablet and on the components. All synchronisation and maintenance tasks, such as configuration changes, event data synchronisation or firmware updates can be performed on all access components within reception range after successful connection. (See also chapter "Carrying out maintenance tasks with a tablet").

You can also use EVVA's special connection cable to connect your access components to the tablet.

The special connection cable can be identified by the EVVA logo on the USB plug. Each access component has a built-in connector interface for synchronising with the Xesar software. The access component's plug interface is located on the front behind the EVVA logo (see chapter "Xesar access components").

Regularly synchronise data using your access components.

The event memory of each Xesar access component stores up to 1,000 events. When the event memory is full, the oldest event entries are overwritten.
By synchronising regularly, you prevent logged events from being overwritten.

Synchronise your Xesar access components at least once a year to keep the Xesar access components synchronised.

If you have installed online components, the data is updated via XVN

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

Close the connector cover again after use to protect the connector interface from dust and moisture!

Do not use pointed objects to open the connector cover!

Please refer to the data sheet for further specifications.

https://www.evva.com/uk-en/xesar/

Functional principle

All maintenance tasks and other tasks for the respective access component are loaded onto the tablet and logged each time the tablet is synchronised with the Xesar software.

Connect the tablet to the access components using a wireless BLE interface or the connecting cable. The data exchange is carried out using the Xesar tablet app (application).

Xesar maintenance app

The Xesar maintenance app is pre-installed on the tablet.

The following features are possible with the Xesar maintenance app:

- Add access components to the system
- Synchronise changed door parameters for Xesar access components
- Transfer blacklist to Xesar access components
- Check current battery status
- Querying the current firmware version
- Perform firmware update
  The battery-powered access component is powered by the tablet during the firmware update. Firmware updates with higher firmware versions than are available in the system can also be carried out in construction mode.
- Transfer events from Xesar access components to Xesar tablet
- Resetting Xesar access component in construction mode
- The access component's time setting is automatically synchronised when it communicates with the tablet.
- Locate BLE access components using identification function

2.6 Emergency power device

Power is supplied to the access component by the emergency power device as necessary. This allows the access component to be operated even when the batteries are discharged.

You need an access medium with a general master key or fire brigade authorisation to open the emergency power-supplied access component, because the time setting will be lost if the power is interrupted for too long.

Emergency power device (sample photo)

» Connect the connection cable from the emergency power device to the connector interface of the corresponding Xesar access component.

» Switch on the emergency power device.

No other interactions with the emergency power device are required. A medium with valid general master key or fire brigade authorisation is required to operate the access component.

» Immediately replace the battery on the Xesar access component after connecting the emergency power supply. Update Xesar access components with the Xesar tablet
This means that access is possible again with all authorised identification media.

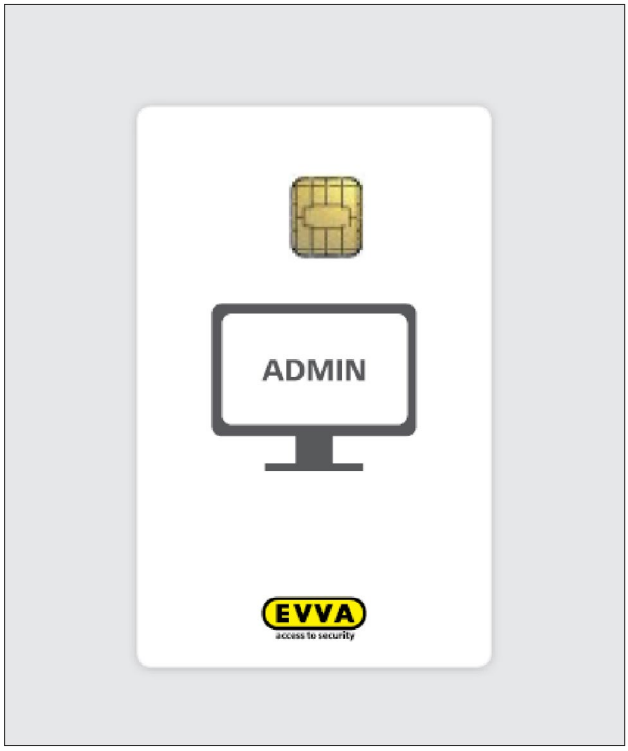
The plug interface built into the access component is only required for the emergency power supply in connection with the emergency power device.

The emergency power device is optionally available.

Option A power supply unit is optionally available for the control unit:
Product code: E.ZU.NG.V1

2.7 Admin Card

The Admin Card is a contact-type, electronic chip card in standard format. The Admin Card permits access to the Xesar software and uniquely identifies the Xesar system.



Admin Card (sample photo)

The KeyCredits required for authorisation changes are stored on the Admin Card. (This does not apply to KeyCredits Xesar Lifetime)

System changes or recharging of KeyCredits is only possible if there is a valid Admin Card in the coding station. The Admin Card is only required for licence operations.

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

The Admin Card can be replaced if it is lost or defective.

2.8 Access media

Access media (cards, key tags, combi keys) are made to open doors or to send system-specific security data between access components and the management software via the virtual network XVN (Xesar Virtual Network).

Access media at a glance

An access media is a non-contact RFID[1]chip-based MIFARE[2] DESFire EV1 with an overall memory capacity of 4 kB.

- Access media are used to open the access components.
  The system must not be in construction mode during this process. In construction mode, the Xesar access component has not yet been electronically assigned to a system. Each Xesar access component as delivered is in construction mode. Access components in construction mode can only be opened with special construction media.

- The coding station is used to program access media.
  To do this, place the access medium on the ready-to-use coding station and carry out the corresponding interactions in the Xesar software.

Do not place more than one identification medium on the Xesar coding station. Thus an incorrect writing of the access media is avoided.

Keep the coding station free of metallic objects so that the reading quality is not impaired.

1 RFID – radio-frequency identification
2 MIFARE – Mikron Fare Collection System (contactless smart card technology)

Please refer to the data sheet for further specifications.

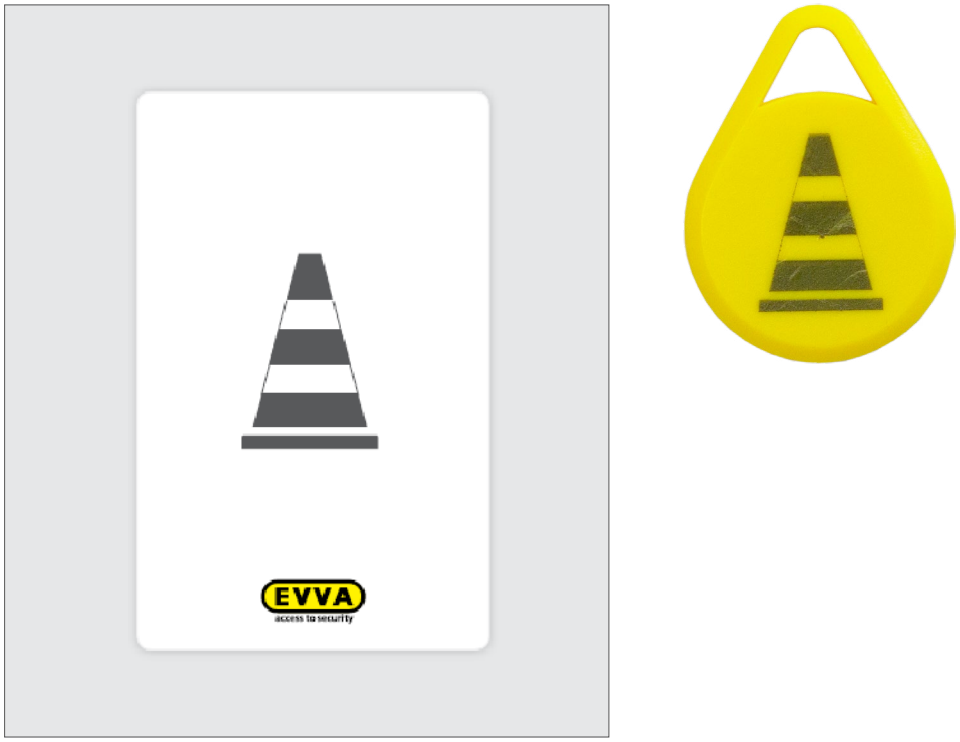
https://www.evva.com/uk-en/xesar/

Number of authorisations per access medium: max. 96 door areas (regardless of the number of installation locations belonging to the area).
Additional 32 installation locations.

2.9 Construction media

Construction media is available in the form of cards and key tags. This allows access components to be opened in construction mode. (In construction mode, the Xesar access component has not yet been electronically assigned to a system. Each access component is in construction mode when delivered).

In addition, the construction media can function as a manual permanent release (see chapter “Time profiles”).



Construction media (sample photos)

The construction card is a contactless smart card equipped with an RFID chip based on MIFARE DESFire EV1.

Your system can be operated in construction mode with any construction media! Therefore, create a system as soon as possible and add your access components.

For efficient commissioning of the system, first create authorisation profiles and their associated areas and time profiles.
Then configure these at the same time as when adding the access components. (See chapter “Commissioning the Xesar software”).

2.10 Bluetooth on/off media

Bluetooth on/off media are available in the form of cards and key tags. The Bluetooth transmitting function of the access component can be activated or deactivated by twice holding the Bluetooth On/Off card on the access component and removing it again. The access component must be in construction mode. The respective transmission status is indicated by visual and acoustic signals. (See also section “Event signalling”.)

The Bluetooth send function can be deactivated for the following reasons:

- usage in Xesar 2.2 or Xesar 3.0 systems
- to extend battery life
- use in radio-sensitive areas

In such cases, access components are maintained using a USB cable.

When BLE components are removed from a system or reset, they remain in the last set BLE transmission mode.

Bluetooth on/off media (sample photos)

This function is only possible with BLE-enabled G2.1 access components.

3 Project checklist and system requirements

3.1 Preface

This document is intended to support the project planning of Xesar 3.2 systems. It consists of 3 parts.

Part 1 is the project checklist, in which important requirements and the new Xesar 3.2 system data are systematically queried and documented for further planning.

Part 2 describes the technical system requirements for a Xesar 3.2 system on PC and for a Xesar 3.2 system on server.

Part 3 includes detailed technical information on the depicted layout and system communication of a Xesar 3.2 system as an appendix.

Use this document as a guide to planning your Xesar 3.2 system.

To clarify the necessary IT infrastructure according to the Xesar 3.2 system requirements, please contact your IT administrator.

If you have any questions about the project checklist or the Xesar 3.2 system requirements, please contact your EVVA Partner or the EVVA technical office.

4 Project checklist

Project title:

Contact persons:

Project:

Phone:

Email:

IT:

Phone:

Email:

System address:

Desired completion date:

4.1 System requirements – infrastructure

System type

Please refer to the following documents for a detailed description of system requirements:

- Xesar 3.2 single-user installation
- Xesar 3.2 multi-user installation

Single-user system: Windows 10 PRO PC type:

Multi-user: Server installation:

- Admin PC: Windows 10 PRO PC type:
- Client PC: Type:
- Server available? Yes / no

  If **yes**:
  Server hardware:

  Server operating system:

  Hypervisor e.g. VMware:

  (See also section 'System requirements to operate a Xesar 3.2 server'.)

  Is the server used only for Xesar? Yes / no
  If **no**:
  What other applications besides Xesar are still running on the server?

System type

New system

Upgrade of existing system Xesar version: X2.2 X3.0

Before upgrading to Xesar 3.2, the existing system must be updated to the Xesar version 2.2 V2.2.38.43 and the latest valid Xesar 2.2 firmware versions must be installed! Furthermore, all open maintenance tasks must be carried out.

Does the existing system feature the 2 wall readers and 1 control unit configuration?

Yes No

Network

WiFi available (requirement for Xesar tablet synchronisation)
Network name: Password:

LAN available

Ports are configurable

(See also section 'System requirements for the network'.)

Backup and data protection are defined and locally available (the responsibility for data backup lies with the operator/user).

Interface requirements

Data transfer or control from third-party system required

Description of the interface requirements:

Interface specification of the third-party system is available

Description:

4.2 System configuration

Desired payment model
(12 and 36-month KeyCredits are not transferable to the Xesar 3.2)

Unit-based KeyCredits (10/50/100) Xesar Lifetime KeyCredits

Number of workstations

Number of workstations with coding station:
(with system and access media management, PC administrator rights required)

Number of workstations without coding station: (System management only)

Number of Xesar tablets: (for maintenance and configuration tasks)

Number of doors planned (installation locations) units

Electronic access components

Escutcheon: Units

Handles: units

Online wall reader: units

Offline wall reader: units

Cylinders: units

Additional components: units

Hybrid system (electronic components and mechanical cylinders)

EVVA system number:

Number of mechanical cylinders: Units

Planned number of access media Units

Cards: Units

Key tags: Units

Combi key: Units

Existing mechanical locking systems
EVVA system number

4.3 Project planning

Installation with several distributed sites (multi-user installation):

Individual or third-party system management of the system (e.g. EVVA Partner, IT service provider):

Server location:

Access system network:

Planned system extensions:

Desired project support:

Frequency with which access authorisations are changed:

Creating lock charts and assigning authorisations:

Checking customer-owned access media (third-party media segmentation):

Fire protection regulations taken into account:

Escape route regulations taken into account:

Privacy requirements (e.g. General Data Protection Regulation) taken into account:

Occupational protection taken into account:

Maintenance and support (maintenance contract):

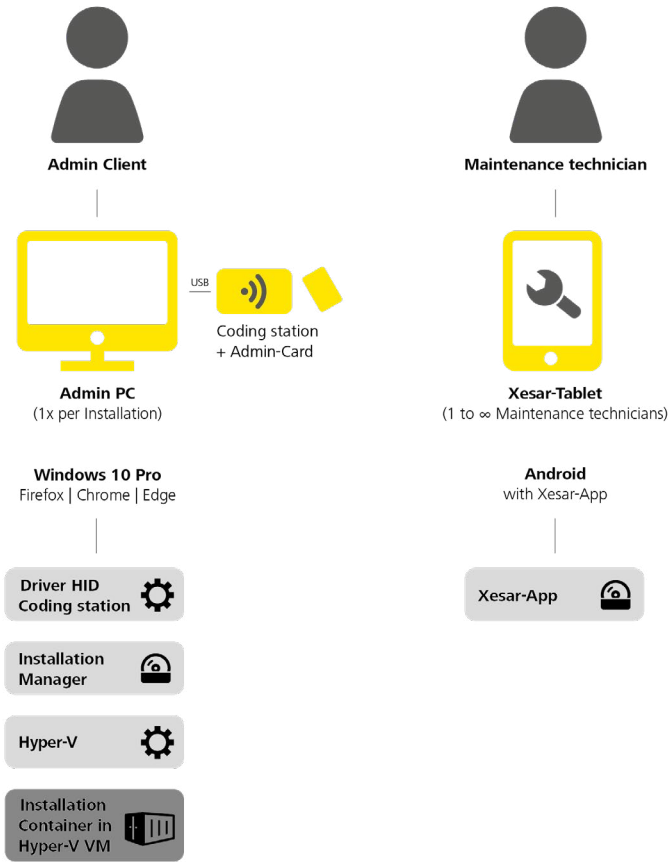
Other agreements:

5 System requirements for single-user and multi-station installations

Xesar can be operated as a single-user installation or multi-station installation. System requirements in the following section.

5.1 Xesar 3.2 single-user installation

24/7 continuous operation and use with online components (e.g. online wall reader) is not recommend for Xesar installations on PC. If the PC for the Xesar installation on PC is not in operation, the online wall reader is in offline mode and access media are not updated. The access system will continue to operate.



The following minimum requirements must be met to operate a Xesar installation on PC:

- x86-64 compatible processor (CPU), at minimum quad core ≥ 1.5-2.3 GHz
- Hardware support for virtualisation
- RAM: ≥ 16 GB (with OS); 4 GB free disk space for installation
- Hard disk space: ≥ 60GB
- Direct Internet access without proxy to unlock KeyCredits and licences to access EVVA secured authentic and unmanipulated software delivery
- Local LAN with low latency (ping <10 ms, roundtrip <30 ms);
  WiFi for Xesar tablet sync and access to the services provided
- 1 × USB Host 2.0
- 1 × EVVA coding station with slot for the admin card and support for contactless Radio Frequency Identification cards (Mifare Desfire EV1; ISO 14443)
- Keyboard and mouse
- Screen resolution: 1920 × 1080 pixels
- Operating system: Windows 10/11 Pro 64-bit
- HTML5/CSS3 compatible browser, with JavaScript enabled
- **Local network:**
  WiFi (wireless): IEEE.802.11 g, n
  Protocols:
  - IPv4
  - HTTP/HTTPS (with TLS)

Services provided by EVVA on the Internet:

Service	URL: Port:	Port addresses
Trusted Registry	https://sfw.evva.com:443 https://sfw.evva.com:4443	Fix
Licence service	https://licence.evva.com:8072	Fix

Service catalogue: Online wall reader communication – server (backend)

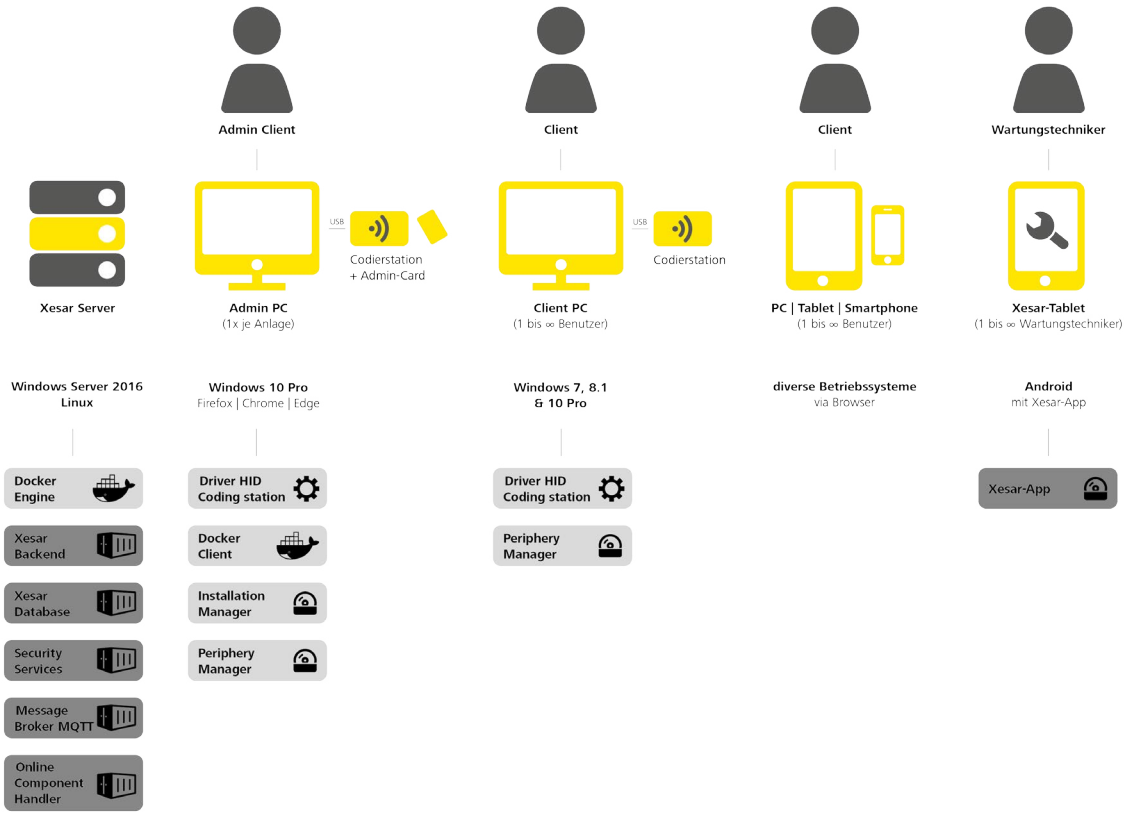
Service	Network	Default port	Port address	Protocols	TLS	Use	Utilising components	Providing component
Online dealership components	LAN/WLAN	9081	configurable	NWP	Yes	Communication with the Xesar software	Xesar online wall reader	Online component dealership

It may be possible to implement the following solutions (please consult EVVA Technical Offices):

- Installation manager operated on a virtual machine
- Installation manager operated on a different Windows operating system
- Use of other browsers compatible with HTML5/CSS3

5.2 Xesar 3.2 multi-user installation

The multi-user installation consists of one **server**, one **admin PC with coding station and admin card,** and potentially other **client PCs with/without coding station**. Optionally, **mobile devices** can also be used via a browser as a client without coding station. The **Xesar tablet** is used as a maintenance tool for installation management. Here is an overview of different variants:



5.2.1 System requirements for multi-user installations

24/7 server operation is required for a multi-user installation. The following minimum requirements must be met:

- x86-64 compatible processor (CPU), at minimum quad core ≥ 1.5-2.3 GHz
- Hardware support for virtualisation
- RAM: ≥ 16 GB (with OS, at least 4 GB for the server software stack)
- Hard disk space, SSD recommended: ≥ 60GB (note system size and planned runtime for dimensioning)
- Direct Internet access without proxy to unlock KeyCredits and licences to access EVVA secured authentic and unmanipulated software delivery
- Local LAN with low latency (ping <10 ms, roundtrip <30 ms)
- WiFI for Xesar tablet synchronisation with the server
- Access option from local LAN to server for provided services
- Docker Engine 1.12.0+ with support for API 1.24 (will be installed as part of Docker installation)

5.2.2 Service catalogue: Management of a Xesar 3 multi-user installation

See section "Server communication"

- Server – admin PC
- Server – client PC
- Server – online wall reader

Tested operating systems

OS	OS type	Version	Virtualisation possible
Ubuntu	Linux	18.04 / 20.04 LTS Server	Yes

Tested Hypervisor

OS	Version	Virtualisation possible
Windows Server	2016 / 2019 Standard / Datacenter	No
VMWare[1]	VMWare ESXi 6.x	No

1 Container optimised operating system recommended by VMware for VMware vSphere ESXi 6.x

Xesar must meet real-time requirements when communicating with its online components. In the event that Windows Server 2016/2019 is not exclusively available to Xesar software, when operating as a hypervisor, it must be ensured that the required resources are permanently allocated.

Due to the large number of possible operating systems not all variants can be tested for compatibility by EVVA.

If an operating system is to be used that is not tested by EVVA, please consult the responsible EVVA Technical Offices beforehand.

Due to the ongoing developments in the IT market, please consult your EVVA Partner or the EVVA Technical Offices with regard to the current compatibility list.

5.2.3 System requirements for administrator PC with coding station and admin card

The following minimum requirements must be met to operate the Xesar software (installation manager):

- x86-64 compatible processor (CPU) 1-2 core, 2.4 GHz or higher
- Support for virtualisation
- RAM: ≥ 16 GB (with OS, at least 4 GB for the applications: installation manager and periphery manager)
- Hard disk space: ≥ 16 GB
- Direct Internet access without proxy to unlock KeyCredits and licences to access EVVA secured authentic and unmanipulated software delivery
- Local LAN to access the services provided by Xesar 3.2 server
- 1 × USB Host 2.0
- 1 x EVVA coding station with support for contactless Radio Frequency Identification cards (Mifare Desfire EV1; ISO 14443) and slot for admin card
- Keyboard and mouse
- Operating system: Windows 10/11 Pro 64-bit
- HTML5/CSS3 compatible browser, with JavaScript enabled
- Docker Client with support for API 1.24, Docker Compose 1.10.0+ (installed as part of the Docker installation on the Admin PC)

5.2.4 Service catalogue: Management of a Xesar 3 system – administrator PC – server

See section "Server communication"

PC operating systems

OS	Version	Browser	Verified by EVVA	EVVA coding station
Windows	10 Pro (V 1511 (build 10586))	Firefox, from version 97.0.1 Chrome, from version 98.0.4758.102 Edge, from version 98.0.1106	Yes	Yes

It may be possible to implement the following solutions (please consult EVVA Technical Offices):

- Operation of the installation manager on a virtual machine on the server (admin card is connected via client PC)
- Periphery manager operated on other operating systems (on request only)
- Use of other HTML5/CSS3 compatible browsers

5.2.5 System requirements for client PC with coding station without admin card

The following minimum requirements must be met to operate a client PC **with coding station** within a multi-user installation:

- x86-64 compatible processor (CPU) 1-2 core, 2.4 GHz or higher
- RAM: ≥ 4 GB (with OS, at least 512 MB for the periphery manager application, 1–2 GB for a supported browser)
- Hard disk space: ≥ 2 GB
- Local LAN with access to the services provided by Xesar 3.2 server
- 1 × USB host 2.0
- 1 × EVVA coding station with support for contactless Radio Frequency Identification cards (Mifare Desfire EV1; ISO 14443)
- Keyboard and mouse
- Screen resolution 1920 × 1080 pixels
- HTML5/CSS3 compatible browser, with JavaScript enabled

5.2.6 Service catalogue: Server and workstations in multi-user installations – client PC – server

See appendix to project checklist 'Client PC communication – server (backend)'

Operating systems

OS	Version	Browser	Verified by EVVA
Windows	7 Pro, 64-bit	• Firefox, from version 97.0.1 • Chrome, from version 98.0.4758.102 • Edge, from version 98.0.1106	Yes
Windows	8.1 Pro, 64-bit		Yes
Windows	10 Pro, 64-bit		Yes

It may be possible to implement the following solutions (please consult EVVA Technical Offices):

- Periphery manager operated on other operating systems (on request only)
- Use of other HTML5/CSS3 compatible browsers

5.2.7 System requirements for client PC without coding station (PC/tablet/smartphone)

The following minimum requirements must be met to operate a client **without** coding station within a multi-user installation:

- x86-64 compatible processor (CPU) 1-2 core, 2.4 GHz or higher
- RAM: ≥ 4 GB (with OS; 1–2 GB for supported browser)
- Hard disk space: ≥ 2 GB
- Local LAN to access the web services provided by Xesar 3.2 server
- Keyboard and mouse
- Screen resolution 1920 × 1080 pixels
- HTML5/CSS3 compatible browser, with JavaScript enabled

5.2.8 Service catalogue: Service catalogue server and work places in multi-user system

See appendix to project checklist 'Client PC communication – server (backend)'

Operating systems

OS	Version	Browser	EVVA tested
Windows	7 Pro	• Firefox, from version 97.0.1 • Chrome, from version 98.0.4758.102 • Edge, from version 98.0.1106	Yes
Windows	8.1 Pro		Yes
Windows	10 Pro		Yes

It may be possible to implement the following solutions (please consult EVVA Technical Offices):

- Comparable browsers on other operating systems (on request only)
- Use of other HTML5/CSS3 compatible browsers

5.2.9 System requirements for network (local network and Internet)

Local network:
- Fast Ethernet 100Base-TX 100 Mbit, standard MTU (1500 bytes) or better
- Low latency between the connected components (ping < 10 ms, roundtrip < 30 ms)
- WiFi (wireless): IEEE.802.11 g, n

Protocols:
- IPv4
- HTTP/HTTPS (with TLS)
- MQTT (with TLS)
- EVVA NWP (with transport lock; online wall reader)

Services provided by EVVA on the Internet:

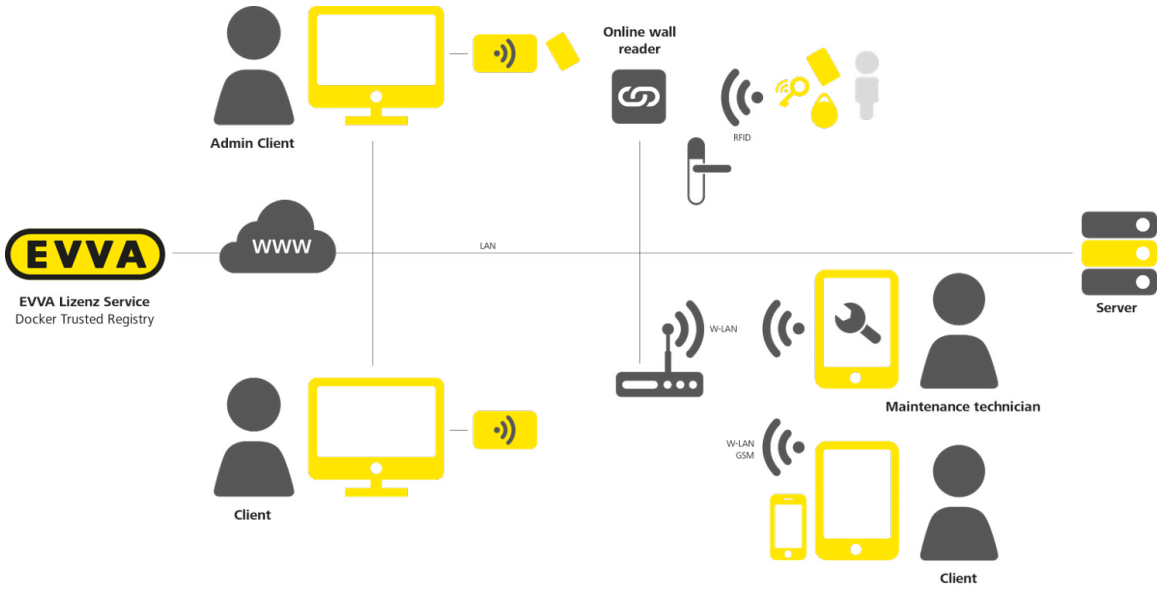
Service	URL	Configurable port
Trusted Registry	https://sfw.evva.com:443 https://sfw.evva.com:4443	No
Licence service	https://license.evva.com:8072	No

Services provided by Xesar 3.2 server within the local network:

Service	URL	What	Configur-able port
Docker Engine	tcp://<IP Installation>:2376	Host	Yes
Security-related service	https://<IP Installation>:8200	Installation	Yes
Message broker	mqtts://<IP Installation>:1883	Periphery, interface	Yes
Management	https://<IP Installation>:8080	Operation	Yes
Online components handler	tcp://<IP Installation>:9081	Operation	Yes

6 Appendix of the project checklist

6.1 Depiction of layout



6.2 Service-communication

Application*)	Service	Network	Default port	Port address	Protocol	TLS	Use	Utilising components	Providing component
1;2	Secure Shell (SSH)	LAN/WLAN	22	Configur-able	SSH	Yes	Setup and configuration of OS and Docker En-gine	Docker Machine, SSH Client	SSH service (OS)
1;2	Docker Engine API service	LAN/WLAN	2376	Configur-able	HTTPS	Yes	Setup the container and volumes	Docker Client	Docker Engine (Docker, OS)
1;2	Message broker	LAN/WLAN	1883	Configur-able	MQTTS	Yes	Asynchronous Xesar system interface	Installation Manager	Message broker
1;2	Service for the management of security information	LAN/WLAN	8200	Configur-able	HTTPS	Yes	Storage for security in-formation, passwords, keys	Installation Manager, installation management	Vault
3	Docker Trusted Registry sfw. evva.com	WAN	443; 4443	443; 4443	HTTPS	Yes	Provision of signed Docker images and verification of the signature	Docker Cli-ent, Docker Engine	Docker Trusted Registry (container image delivery)
4	Licence service licence.evva. com	WAN	8072	8072	HTTPS	Yes	Register-ing an In-stallation/ AdminCard and loading key-credit codes	Xesar Installation Manager	Licence service
5	AdminCard Terminal	USB	Fix	–	ISO 14443	–	Reading and writing of identification media	Installation management via the Periphery Manager (proxy only)	Coding station

Application*)	Service	Network	Default port	Port address	Protocol	TLS	Use	Utilising components	Providing component
6	Installa-tion and management of frontend Web Service	LAN/WLAN	8080	Configur-able	HTTPS	Yes	Web service and delivery of the web application for the browser	Browser	
7	Online dealership components	LAN/WLAN	9081	Configur-able	NWP	Yes	Communi-cation with the Xesar software	Xesar online wall reader	Online component dealership

*) **Applications:**

Admin PC with Xesar Installation Manager
1: System start
2: System stop
3: System update
4: Licence service (KeyCredits loading)
5: with coding station for AdminCard

Client PC
5: Coding station for identification media
6: Client PC Browser-Communication

Online wall reader
7: Online wall reader communication

6.3 Communication Client PC – Server (backend)

Service	Network	Default Port	Port address	Protocol	TLS	Use	Utilising components
Installation and management of frontend Web Service	LAN/WLAN	8080	Configurable	HTTPS	Yes	Web service and delivery of the web application for the browser	Browser
Message broker*	LAN/WLAN	1883	Configurable	MQTTS	Yes	Asynchronous Xesar system interface	Periphery Manager
Coding station*	USB	Fix	–	ISO 14443	–	Reading and writing of identification media	Installation management via the Periphery Manager (proxy only)

* Only for Client PC with coding station

6.4 Communication, Online wall reader – Server (backend)

Service	Network	Default Port	Port address	Protocol	TLS	Use	Utilising components	Providing component
Online dealership components	LAN/WLAN	9081	Configurable	NWP	Yes	Communication with the Xesar-Software	Xesar online wall reader	Online component dealership

7 Upgrade und Updates

An upgrade to Xesar 3.1 is only possible from systems with Xesar 2.2 and Xesar 3.0.

This applies for both firmware and software.

The following requirements apply for upgrades to Xesar 3.1:

Xesar-Software
PC's operating system: Windows 10 Pro

Xesar tablet
WLAN is required

After installing, the Xesar
access components must be updated with the new firmware

Xesar wall reader
Procedure for configuration of a "control unit and two Xesar wall readers":

- Remove the Xesar wall reader from the system and reset it to construction site mode
- After installing Xesar 3.1, add the Xesar wall readers to the system.

AdminCard
The X2.2 card must be used as the AdminCard

	**Access media** After the upgrade, media from X2.2 systems must be upgraded at the online wall reader or coding station.
	**KeyCredits** Lifetime and KeyCredits balances are transferred. KeyCredits Unlimited 12/36 months are lost.

Xesar 3.1 supports the following tablets:

Xesar tablet V2 (Acer Iconia One 7 (B1-770 and B-730HD)
Restricted functions: no BLE function, only cable connection possible

Xesar Tablet Ares BLE 4.2
Full function, BLE and cable connection

8 Upgrade Xesar 2.2 to Xesar 3.1

The operation of the Xesar software 3.x differs significantly from the operation of the Xesar software 2.2.
We therefore strongly recommend attending a comprehensive training course at our EVVA Academy before migrating from Xesar 2.2 to Xesar 3.x.
You can obtain training dates from EVVA Support.!

When upgrading Xesar 2.2 installations to Xesar 3.1, please note the following points:

8.1 Before upgrading

- A Xesar 2.2 system can only be imported and operated in the same time zone.
- The existing AdminCard from your Xesar 2.2 system will continue to be used.
- Existing access media can continue to be used. For this purpose, you must update them at the coding station or an online wall reader.
- KeyCredits can continue to be used.
- KeyCredit Unlimited (12 or 36 months) can no longer be used with Xesar 3.x, they will expire!
- Use KeyCredit Xesar Lifetime for unlimited use and pay only once!
- The Xesar Lifetime licence may only be activated after the upgrade to Xesar 3.1 has been completed.
- Carry out all outstanding maintenance tasks on your Xesar 2.2 system.
- Create a manual backup of your Xesar 2.2 system for security reasons.
- Take screenshots of Xesar 2.2 event logs.
  Event log data cannot be transferred or imported from Xesar 2.2 to Xesar 3.0.
- If you use the configuration “Two Xesar wall readers with one control unit” in your Xesar 2.2 system, these wall readers must be disconnected from the Xesar 2.2 system and put into construction site mode before upgrading to Xesar 3.x.
  After upgrading to Xesar 3.1, install the two wall readers in the system again.
- The ports required by Xesar are both free and available. 8080, 1883, 8200, 9081. The firewall must not block the required ports. If necessary, you can change the ports at a later point in time.
- Uninstall the existing Xesar maintenance app on your Xesar tablet. After the successful upgrade, the new Xesar maintenance app 3.1 must be manually installed on the Xesar tablet (see chapter “Manually uninstalling and installing the Xesar maintenance app”).
- If a Xesar 2.2 system with a fire brigade authorisation profile is imported into Xesar 3.1, it is possible that a second fire brigade authorisation profile is created. In this case, a fire brigade authorisation profile must be removed manually.
- After a Xesar 2.2 system has been imported into Xesar 3.1, the components can no longer be synchronised with the Xesar 2.2 system and can only function under Xesar 3.1.

- After the upgrade, maintenance tasks for the firmware update are generated for all components. The current Xesar 3.1 component firmware is transferred to the components using the Xesar tablet and the current Xesar maintenance app.
- To ensure the functional safety of the system, carry out these maintenance tasks as soon as possible after the upgrade.

8.2 Upgrade instructions Xesar 2.2 to Xesar 3.1

» Stop the Xesar 2.2 installation.
» Install the new Xesar 3.1 Installation Manager (see Xesar 3.1 Installation instructions).
» Insert the AdminCard from your Xesar 2.2 system into the coding station.
» Select “Restore/Import” under PC systems in Xesar 3.1 Installation Manager
» Load the Xesar 2.2 database file and follow the instructions. You can find the Xesar 2.2 database file at:
C:\ProgramData\Xesar 2.2\<Nummer der Admin-Karte>

After the successful upgrade, you will find your system under PC systems.

For help and further information, please contact your EVVA partner or the EVVA technical office.

9 Instructions for upgrading a Xesar 3.0 PC system to Xesar 3.2

For Xesar 3.0 systems on servers, please contact your EVVA support team before updating

View Xesar systems on PC:
PC systems installed with the new Installation Manager are displayed and managed here. PC systems can be moved from the Server systems view to the PC systems view.

View Xesar systems on server:
The display is identical to that of the Xesar 3.0 Installation Manager. Systems that have been updated by Xesar 3.0 are displayed here.

9.1 Update steps on the PC

- Create a current backup file in the existing Installation Manager by means of a manual backup.
- Exit the old Installation Manager.
- Install the new Installation Manager.
- Insert the AdminCard from your Xesar 3.0 system into the coding station.

You will find your Xesar system under Server systems.

- Remove the system from the Server systems view.
- Go back to the start page of the new Installation Manager.
- Click on Restore/Import in the PC System View. Then import the most recent Xesar 3.0 system backup file.
- Follow the installation steps.

After the successful update, you will find your system under PC systems.
The further administration of your installation takes place under the PC systems view.

9.2 Update steps on tablet

» Uninstall the existing Xesar maintenance app on your Xesar tablet.

» After successfully updating, install the new Xesar maintenance app 3.2 manually on the Xesar tablet (see chapter “Manually uninstalling and installing the Xesar maintenance app”).

In Xesar 3.2, the local Docker installation is no longer required and can be uninstalled after a successful update.

For help and further information, please contact your EVVA partner or the EVVA technical office.

10 Installation instructions

10.1 Installing the coding station driver

The HID hardware driver must be installed in order to operate the coding station (HID Omnikey 5421) on the PC.

If you have the HID Omnikey 5422 version of the coding station, driver installation is not necessary. (In this case, continue directly to chapter “Xesar 3.2 Programmes”).

The following alternatives are available for installing the driver for the coding station:

- Automatic driver search in Windows
- Manual search for driver on the manufacturer’s homepage

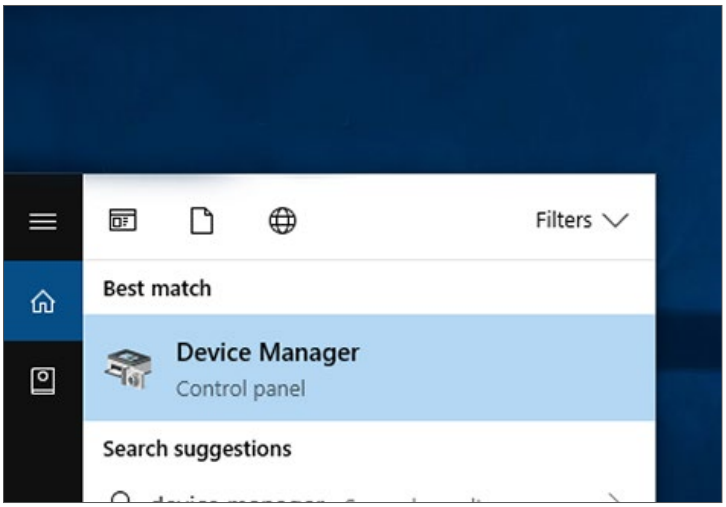
10.1.1 Automatic driver search

Windows 10 usually detects the coding station automatically. The plugged-in coding station is checked during installation on a PC

Please use the Windows Device Manager to install the coding station's driver.

» **1. Step:**
Plug your coding station without an AdminCard into the USB port of your PC!

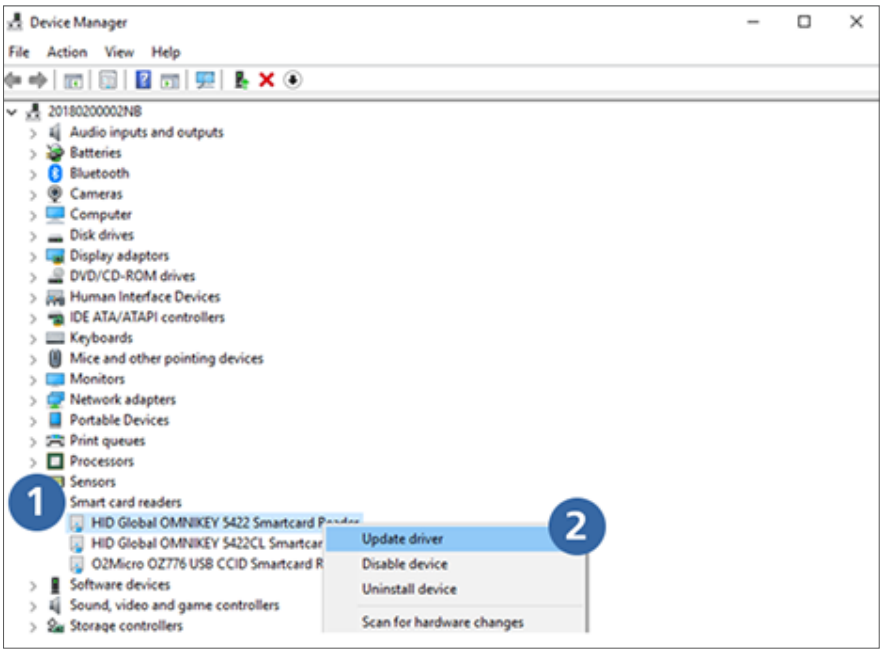
» **2. Step:**
Open the “Device Manager” via the Windows search bar.



» **3. Step:**

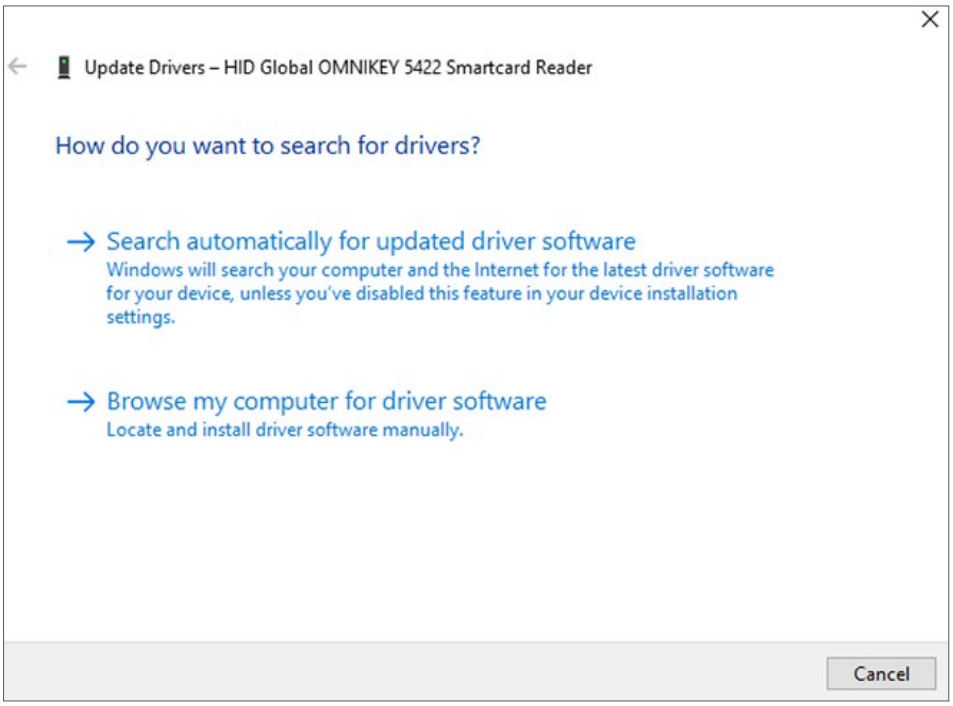
❶ Search the list for **Smartcard Reader** (or Reader).
Open with a mouse click and select the item that begins with **Microsoft ...**.

❷ Right-click on the entry **Microsoft...** and select **Update driver**.

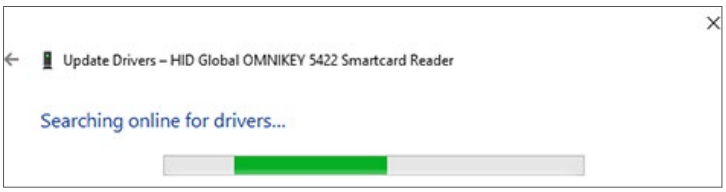


» **4. Step:**

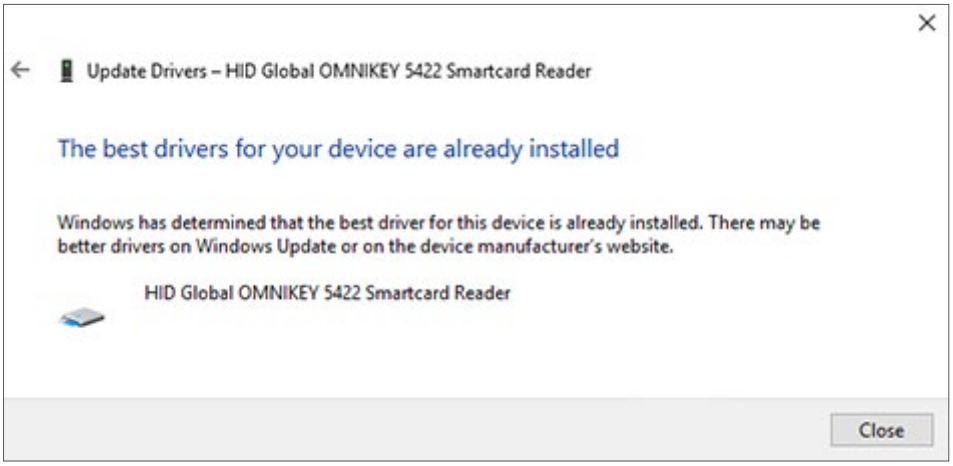
Confirm the message **automatically search for updated driver software**.



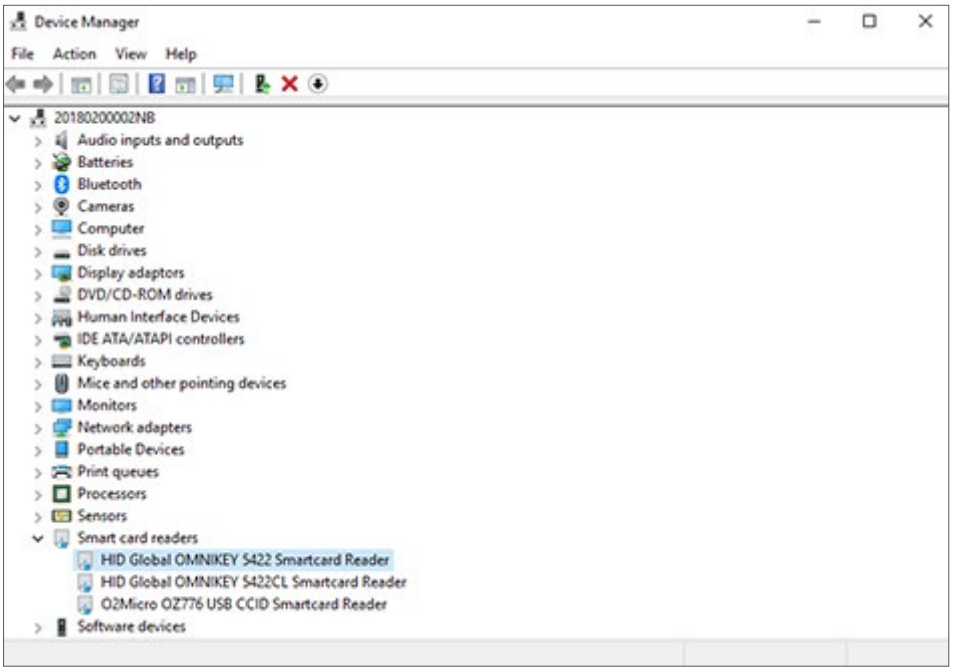
» **5. Step:**
The driver is downloaded and installed automatically!



» **6. Step:**
The driver has been installed. Click **Close**.



The Omnikey 5x21 reader used is now listed in the Device Manager.



The installation of the coding station driver is now complete. As a next step, proceed to chapter “Xesar 3.2 Programmes”.

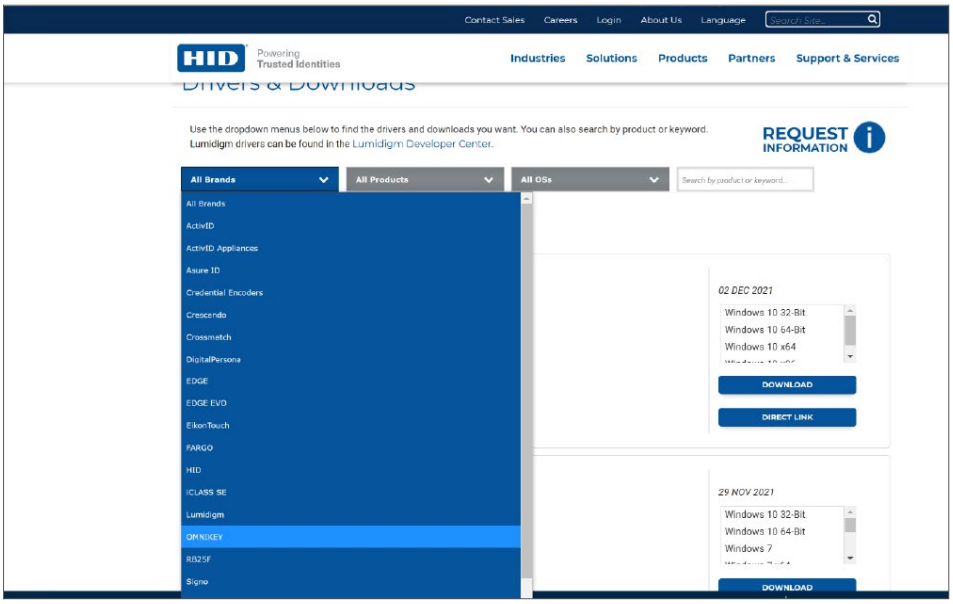
10.1.2 Manual driver search

As an alternative to the automatic driver search, it is possible to download the correct driver directly from the HID Global site.

» **1. Step:**
Verify the model type of your Omnikey coding station (on the rear of the device, e.g. HID OMNIKEY 5421) and plug the coding station into your PC.

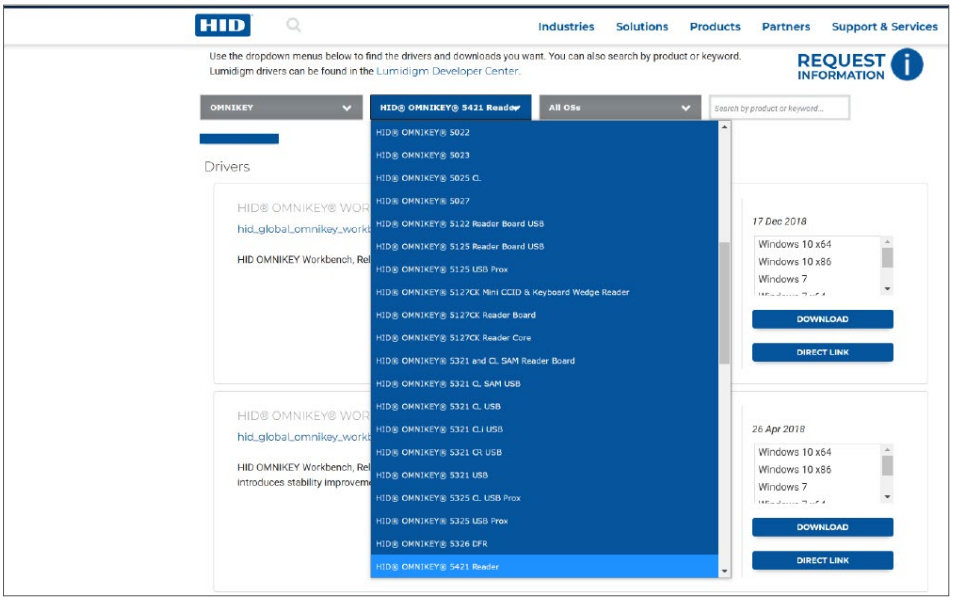
» **2. Step:**
From your browser, go to the HID Global website and launch the Driver website:

› **https://www.hidglobal.com/drivers**



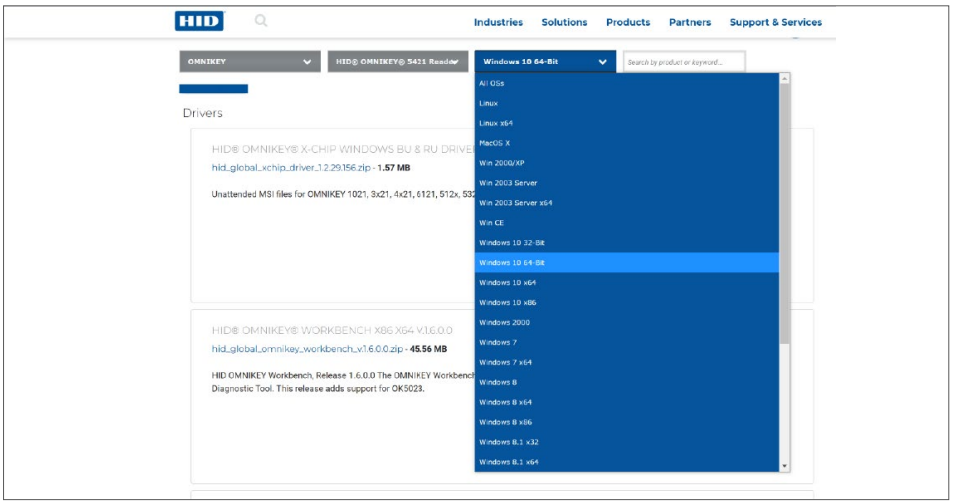
3. Step:

Select your model (e.g. HID OMNIKEY 5421)



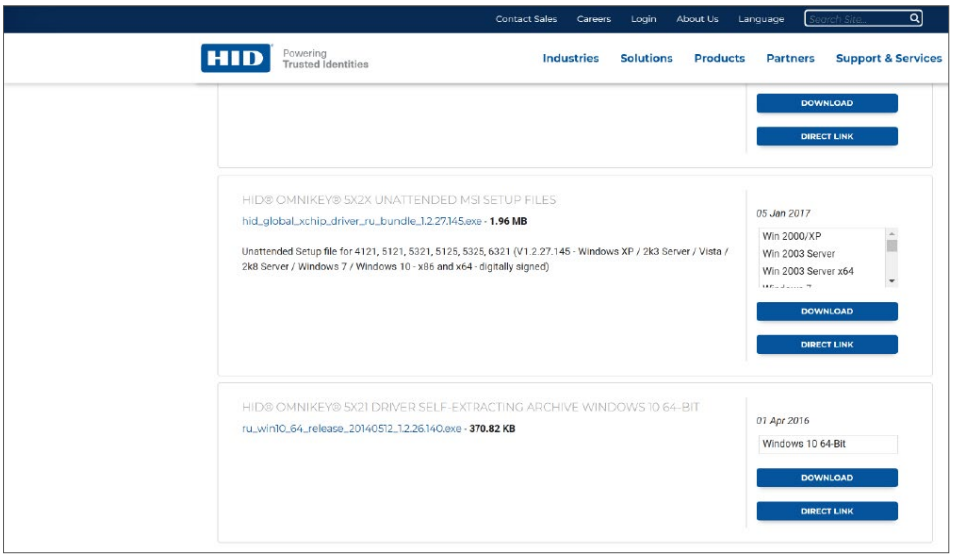
4. Step:

Select your **64 bit Windows 10** operating system.



Select a driver from the list.

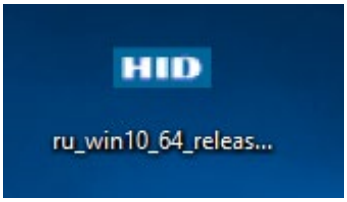
» **5. Step:**
Scroll to the driver named “Self-extracting archive” for 64 bit Windows 10 systems and click **Download**.



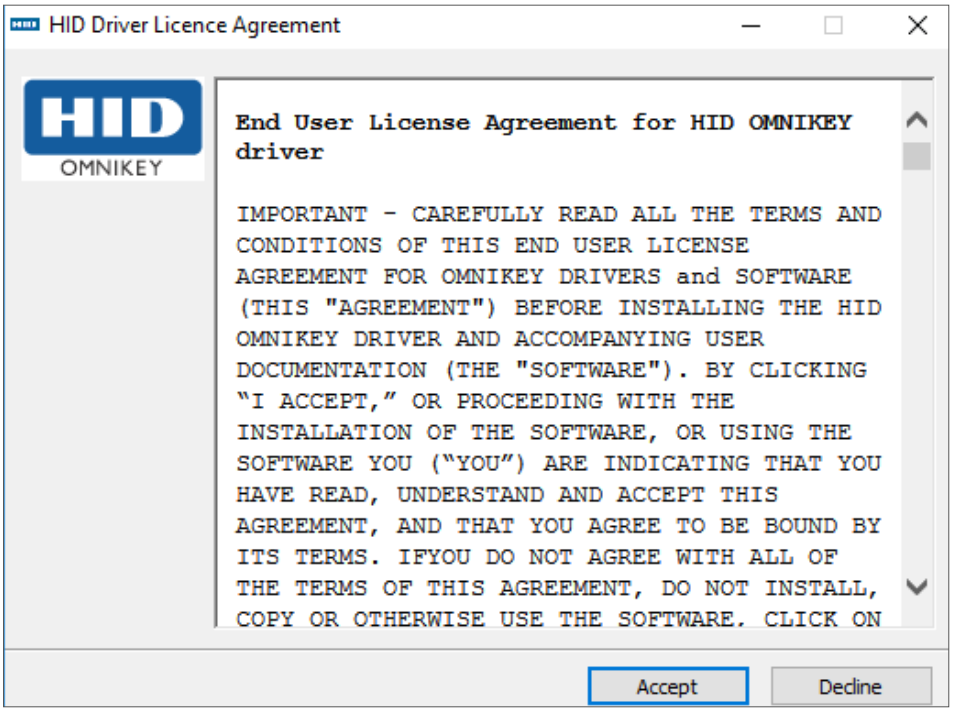
If the message “Download EULA” (End User Licence Agreement) appears, confirm your acceptance. The download begins.

You can open the file in your browser (via “Run”) and start the installation process - in this case, go to the 7. Step:

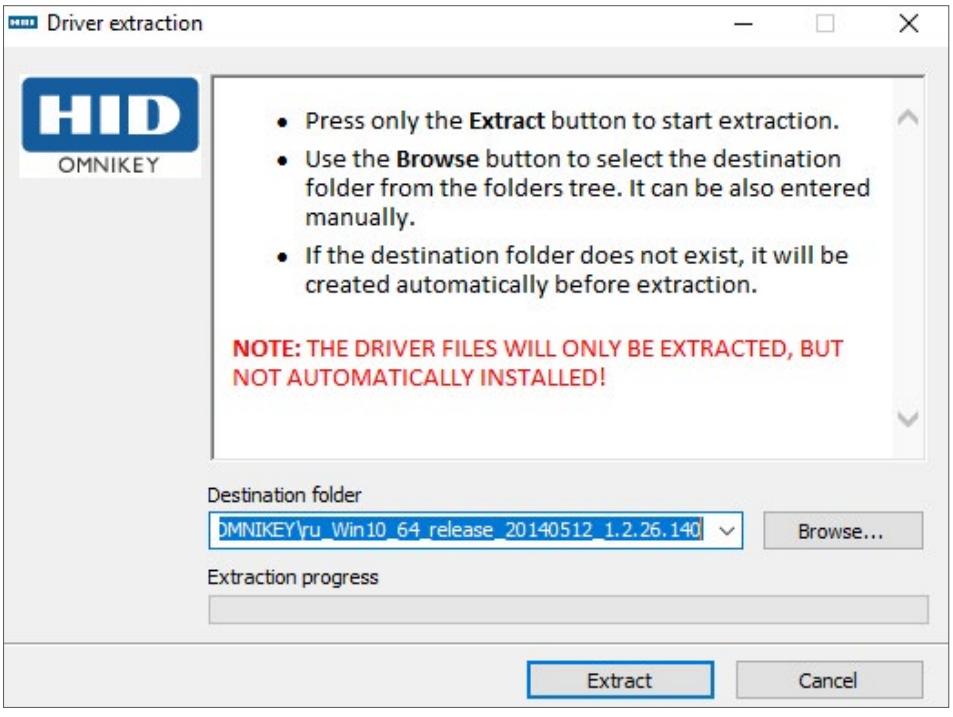
» **6. Step:**
Double-click on downloaded file



» **7. Step:**
Confirm that you accept the message "HID Driver Licence Agreement"



» **8. Step:**
The "Driver extraction" window opens - click on **Extract** to install the driver.



When the 8th step is complete, you have successfully installed the HID driver.

11 Installation instructions for server with Ubuntu 22.04

The following provides information on preparing the Xesar 3.2 installation on a server that uses the Ubuntu 22.04 operating system.

The creation of the necessary IT and server environment is not part of these installation instructions. It must be provided by the customer and is not the responsibility of EVVA.

» Check the system requirements for Xesar 3.2. **Before installation, you must confirm that the system requirements for Xesar 3.2 are met in accordance with the project checklist and system manual.**

Follow the current project checklist from EVVA:

› **https://www.evva.com/uk-en/xesar/**

We strongly recommend that you only carry out the Xesar 3.2 installation in close cooperation with the customer's responsible IT administrator.

11.1 Requirements

The following requirements must be met for successful installation of Xesar 3.2 on a server with the Ubuntu 22.04 LTS Server operating system:

- Xesar Admin PC now called “Windows Admin Client” WIN 10/11 PRO with Installation Manager
- Server with Ubuntu 22.04
- Xesar 3.2 system requirements are met
- Supported hypervisor for virtualisation: VMWare and Windows Server from 2016. Nested virtualisation is not supported here.

11.2 Installing Ubuntu

The following instructions apply to 22.04

» Download Ubuntu 22.04

› **http://releases.ubuntu.com/**

Tutorial for Ubuntu installation

› **https://tutorials.ubuntu.com/tutorial/tutorial-install-ubuntu-server#0**

Bootable USB stick

› **https://tutorials.ubuntu.com/tutorial/tutorial-create-a-usb-stick-on-windows#0**

» Follow the instructions during the installation

» While installing Ubuntu, select **open ssh server** during the final installation step.

If this option is not available, it can be installed afterwards in the Linux Console with the command **sudo apt install openssh-server**. If "sudo without password" (see below) has not yet been configured, then the user password will be requested.

» To set up sudo without a password, enter the following commands into the Linux Console:

  » Enter the command **sudo visudo** for the password prompt for sudo (Password is requested and the file /sudoers.d will open)

  » Scroll to the end of the opened file and type the command **username ALL=(ALL) NOPASSWD: ALL** below the final line:

```
@includedir /etc/sudoers.d
shqadmin ALL=(ALL) NOPASSWD: ALL
```

» Save file (Ctrl+O and then ENTER)

» Close file (Ctrl+X)

» Check that the command **sudo visudo** now works without a password.

» In the Linux console, create an **SSH keypair** using the command **ssh-keygen -t ed25519**.

```
shqadmin@test:~$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/shqadmin/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/shqadmin/.ssh/id_ed25519
Your public key has been saved in /home/shqadmin/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:/gxqd3yA/mdFKVLce154ADDkzQO7+FcIVT6ZA2BkYxk shqadmin@test
The key's randomart image is:
+--[ED25519 256]--+
|          .=EB=...|
|          .+*+=+oo|
|           o.= oXo|
|           ....=.*|
|        S. ..o.+.|
|       .. .  .. .|
|       .o. . .   |
|      ..o+o +    |
|     ... o++     |
+----[SHA256]-----+
```

The ssh key is stored by default at /home/user/.ssh on the Linux server.
In our example, the user is **shqadmin**, which we created when setting the Linux installation.

In the next step, you need to add the public key (.pub) in the Linux console of the key pair created to the authorised keys on the Linux server.

» Using the first command line, go to the previously created directory

» Using the second line, add the key:

  » **cd /home/user/.ssh**

  » **cat id_ed25519.pub > authorized_keys**

```
shqadmin@test:~$ cd /home/shqadmin/.ssh
shqadmin@test:~/.ssh$ cat id_ed25519.pub > authorized_keys
```

» Install Docker:

  » **sudo apt install docker.io**

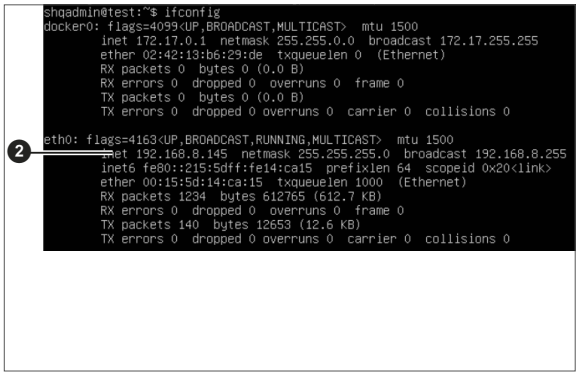
» Install a program (e.g. putty or WINSCP) on the Windows Admin Client to transfer data securely from the client to the server and vice versa.
In our example, WINSCP is used.

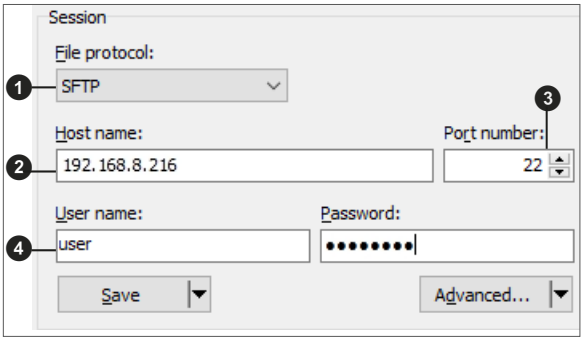
Freeware program

https://winscp.net/eng/download.php

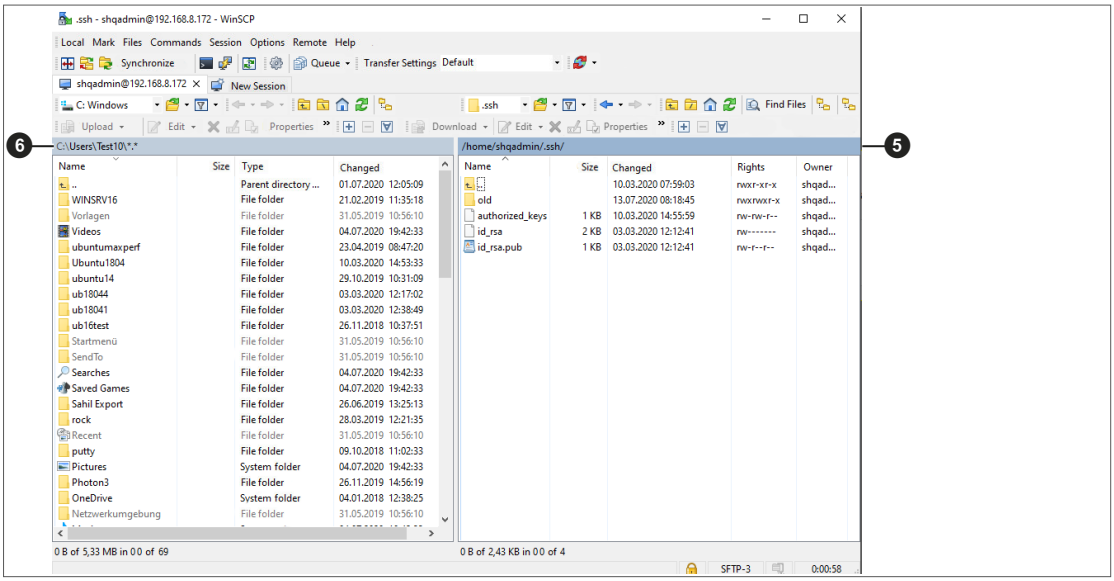
» Log in using WINSCP on the server

Transfer protocol ❶ is SFTP
Computer name ❷ is the IP address of the server (can be found in the Linux console with the command **ifconfig**)
Port ❸ is 22 (standard)
User and password ❹ correspond to the user and their password on the Linux server





» Copy the private key **id_ed25519** to the Windows Admin Client using WINSCP. (In our example from /home/shqadmin/.ssh ❺ on the server to C:/ Program Files\EVVA\Xesar3 Installation Manager 2.0\runtime\bin ❻to the Windows Admin Client



» Open the Windows Console

(with **cmd** in search, right-click as Admin)

» Use the command **cd C:/Program Files\EVVA\Xesar3 Installation Manager 2.0\runtime\bin** in the Windows Console to change the directory where the private key id_ed25519 was stored

11.3 Create Docker Machine

» Enter the command to create the Docker Machine in the Windows Console (also from the directory in which the private key is located)

```
C:\Users\Administrator>cd C:\Program Files\EVVA\Xesar3 Installation Manager 2.0\runtime\bin

C:\Program Files\EVVA\Xesar3 Installation Manager 2.0\runtime\bin>docker-machine --debug create --driver generic
 --generic-ip-address 192.168.8.10 --generic-ssh-key id_ed25519 --generic-ssh-user shqadmin hostname
```

The general command is:

docker-machine create --driver generic --generic-ip-address (IP server address) --generic-ssh-key (name of the public key) --generic-ssh-user (name of the user for whom the Ubuntu server was created) (name of the Docker Machine)

Command part	Explanation
docker-machine create	is the general command to create a Docker Machine
--driver generic	is the generic driver for installing Docker on the server
--generic-ip-address	is the IP address of the server
--generic-ssh-key	is the description of the private key used. (If executed from the directory in which it is stored. For a different directory, the entire path must be entered.)
--generic-ssh-user	is the description of the ssh user (“shqadmin” in our example). After a space, this is followed by the name of the Docker Machine (xs3ubuntu1804 in our example).

The whole docker-machine create process takes approx. 2 to 10 minutes, depending on the computer.

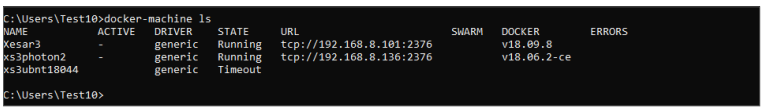
If an unexpected error message occurs, you can cancel the process by exiting the Windows Console.
Then reopen the Windows Console and delete the incorrectly set up Docker Machine with the command docker-machine rm „name“ (name is the assigned name).
Example: docker-machine rm xs3ubuntu1804

» Then enter the command **docker-machine --debug create --driver generic --generic-ip-address (IP address of the server) --generic-ssh-key (name of the public key) --generic-ssh-user (name of the user for whom the Ubuntu Server is created) (name of the docker machine).** Use the extension --debug to obtain a precise error report.

If an error message relates to the **ssh connection**, check the user again with **sudo** without password or check the storing of the **ssh-keys**.

Another source of error with regard to ssh is the folder C:\Windows\System32\OpenSSH. In the event of an error (ssh exit status), rename it to ...**old**OpenSSH.

» After successfully creating the Docker Machine, use the command **docker-machine ls** in the Windows Console to check whether the Docker Machine is running.

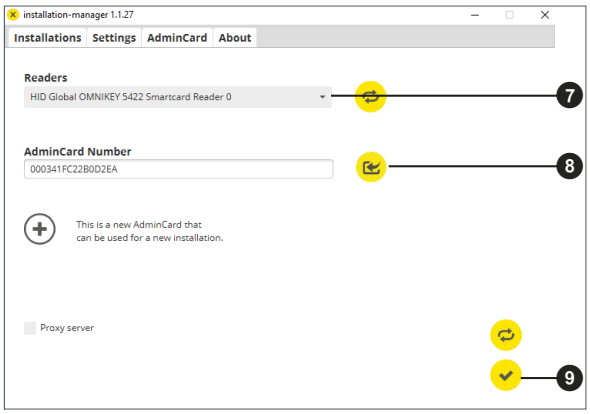


11.4 Xesar 3.2 installation

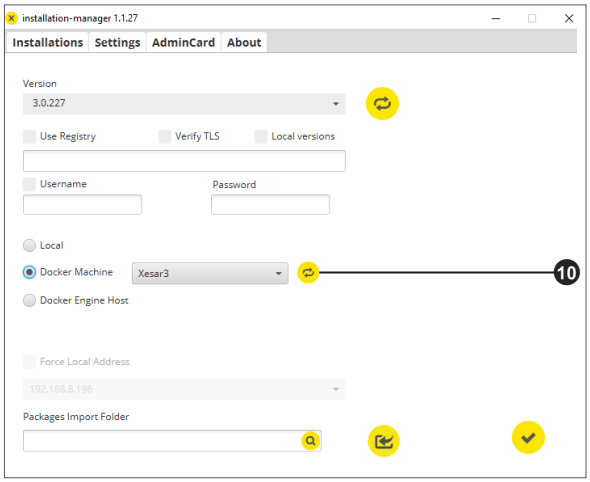
- Download the latest Xesar 3.2 software

  https://www.evva.com/uk-en/products/electroniclockingsystem-saccesscontrolsystems/xesar/download-xesar-software/

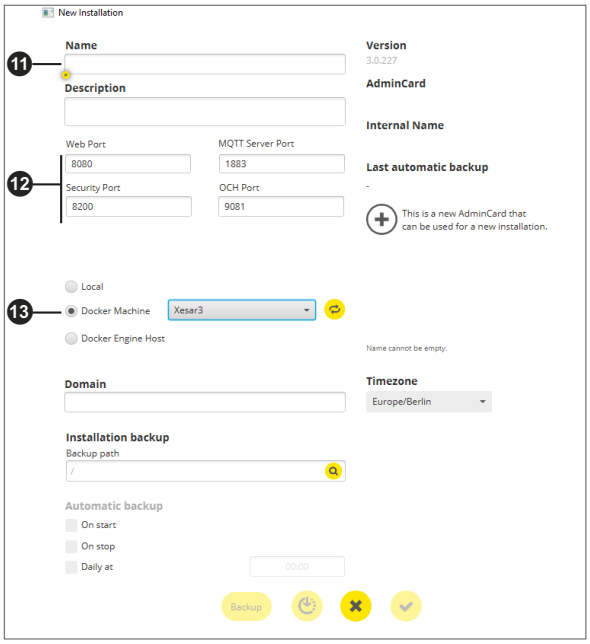
- Connect coding station
- Start the Installation Manager
- Select Manage Xesar installations on server → Manage installations
- Select the tab Admin Card
- Select the required card reader ❼
- Load the Admin Card ❽
- Click on the button ❾to read in the number of the Admin Card



- Select the tab Configuration
- Select the Docker Machine ❿



- Select the tab **Installations**
- Using the "+" button, add a new system
- Select the name ⓫, the port ⓬ and the Docker Machine ⓭



If you are updating Xesar 2.2, enter the database path for the import. After creating the system, you can start and commission the system (see system manual).

11.5 Data backup

The following data must be saved:

- Backup from the Installation Manager (Installation → pen symbol → Backup)

- **Windows Admin Client**
  [XesarUser] is a placeholder for the Windows user (e.g. admin) who performed the Xesar 3.2 installation

  - C:System\Users\[XesarUser]\.xesar
  - C:System\Users\[XesarUser]\.xesar-cs
  - C:System\Users\[XesarUser]\.docker
  - ssh key

Manual and automatic data backups (backup) can be performed in the Installation Manager.

- **VM server**

  - Snapshot of the VM after each large or important change
  - Generally a mirroring of the whole partition, preferably the whole hard drive on which the Xesar VM (for example Ubuntu) is installed – as is usual with servers
  - ssh key

- **Physical server**

  - entire hard drive

12 Installation Instructions Windows Server 2019 Datacenter Hypervisor

You will find information below on how to prepare the Xesar 3.2 installation on a Windows server that uses the Windows Server 2019 Standard operating system versions or Datacenter as hypervisor.

The creation of the necessary IT and server environment is not part of these installation instructions. These must be provided by the customer and is not the responsibility of EVVA.

» Check the system requirements for Xesar 3.2. **Before installation, you must confirm that the system requirements for Xesar 3.2 are met in accordance with the project checklist and system manual.**

Follow the current project checklist from EVVA:

› **https://www.evva.com/uk-en/xesar**

We strongly recommend that the Xesar 3.2 installation is only carried out in close cooperation with the customer's responsible IT administrator.

12.1 Requirements

A physical server is setup with Microsoft Windows Server 2019 and configured as a hypervisor. On this a VM with current Ubuntu LTS server is installed on which Docker with Xesar 3.2subsequently runs.

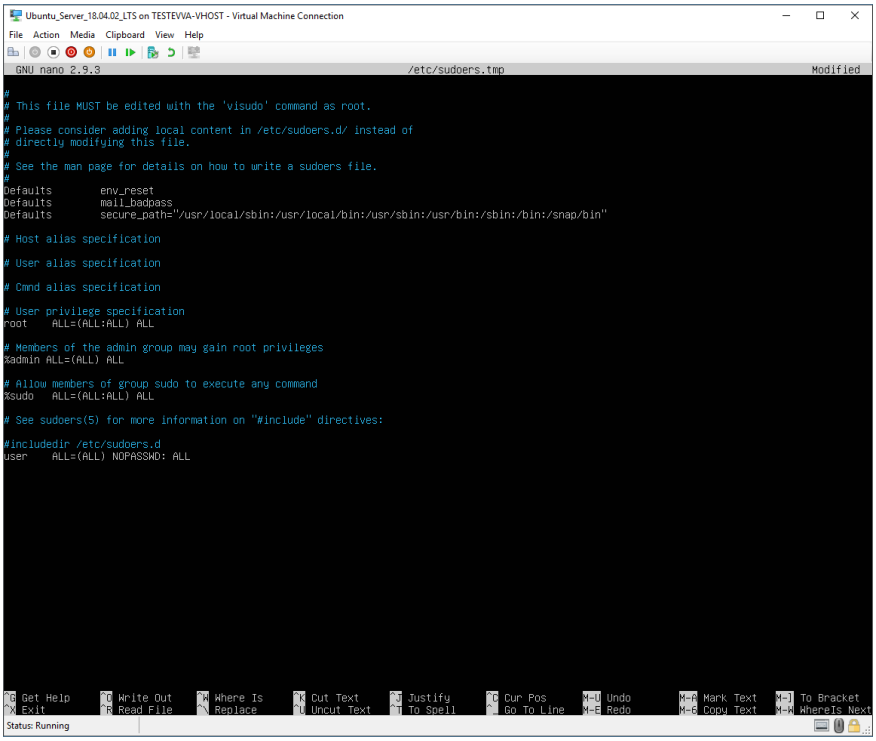
The following requirements must be met for a successful installation of Xesar 3.2 on a server running the Windows Server 2019 operating system:

- A physical server with an installed Windows Server 2019 / Datacenter operating system, from version 1607
- Configuration as hypervisor for VM (virutal machine) for Ubuntu LTS Server for Docker
- The user (customer) has Windows Server and network administration expertise
- The user (customer) has local administration rights
- There is an existing DHCP service (Dynamic Host Configuration Protocol)
- The Server time zone is set to UTC (Coordinated Universal Time)
- A Hyper-V support must be available, as well as a virtual switch with connectivity and access to the Internet
- Internet access must be available (Docker Trusted Registry with Notary Service and Licence Service, Port 443, 4443, 8072)
- The driver for the coding station must be installed, if necessary (HID Omnikey 5422 is usually detected automatically)

Due to the resource availability associated with the Windows Server, we recommend 16 GB (min. 8 GB) for the physical server. The VM requires at least 4 GB of memory.
As a general rule, the larger the system and the more people / traffic and online wall reader, the more memory should be available.

12.2 Set up Ubuntu

- Enter command **sudo visudo** for the password prompt for sudo
- At the following line to the end of the file that has now opened:
  user ALL=(ALL) NOPASSWD: ALL
- Replace the underlined word with the name of the user specified during the installation



- Save file (Ctrl+O and then ENTER)
- Close file (Ctrl+X)

» Create SSH key pair with **ssh-keygen** command. Name and password can be left blank - confirm with ENTER

```
shqadmin@ubuntumax:~$ ssh-keygen -t ecdsa -b 521
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/shqadmin/.ssh/id_ecdsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/shqadmin/.ssh/id_ecdsa
Your public key has been saved in /home/shqadmin/.ssh/id_ecdsa.pub
The key fingerprint is:
SHA256:Y/IE6YgmH6qzn/Qh1ync9LTBlyBoyhT/ODri0DvTvPs shqadmin@ubuntumax
The key's randomart image is:
+---[ECDSA 521]---+
|  .              |
|   o . .         |
|  . + + .        |
| o + = + . .     |
|. * + = S o      |
| * + = O =       |
|+ Bo= + +        |
|=ooBoo           |
```

» Add the SSH Public Key to the authorised keys:

  » **cd /home/user/.ssh/**

  » **cat id_ecdsa.pub > authorized_keys**
  cat id_ed25519.pub > authorized_keys

» Replace the underlined word with the name of the user specified during the installation

```
shqadmin@ubuntumax:~$ cd /home/shqadmin/.ssh
shqadmin@ubuntumax:~/.ssh$ cat id_ecdsa.pub > authorized_keys
```

12.3 Install Ubuntu updates

Download and install the latest updates and then restart with the following commands:

» **sudo apt-get update**

» **sudo apt-get upgrade**

» **sudo apt-get dist-upgrade**

» **sudo apt-get autoremove**

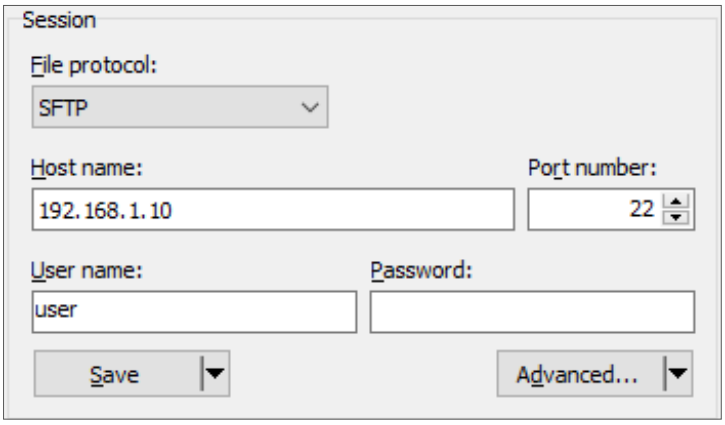
» **sudo reboot now**

12.4 Set up Windows 10 Pro Administrator PC

» Download and install WINSCP (Windows Secure Copy) to transfer the SSH key

› https://winscp.net/eng/download.php

» Start WINSCP
To do this, you will need the computer name, port, usernames and the password of the Ubuntu server that was previously set up.



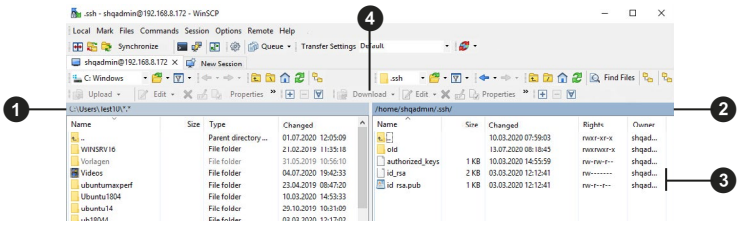
» Display the files and folders cached in WINSCP (Ctrl+Alt+H)

» Go to a folder on the local Windows PC (on the left ❶).

» Go to the Ubuntu server in the ".ssh" folder on the right ❷

» Select the files "id_rsa" und "d_rsa.pub" ❸

» Click on **Download** ❹ to download the selected files onto the Windows PC.



» Then download and install the latest version of Docker CE

› https://docs.docker.com/docker-for-windows/release-notes/

» Restart Windows PC

» Check installation.

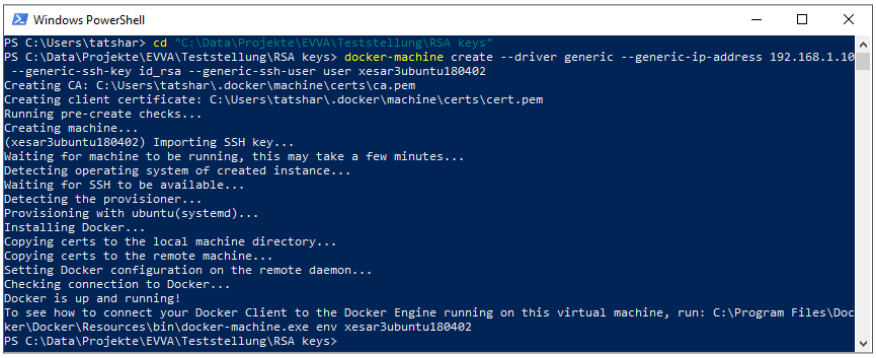
```
PS C:\Users\tatshar> docker version
Client: Docker Engine - Community
 Version:           18.09.2
 API version:       1.39
 Go version:        go1.10.8
 Git commit:        6247962
 Built:             Sun Feb 10 04:12:31 2019
 OS/Arch:           windows/amd64
 Experimental:      false

Server: Docker Engine - Community
 Engine:
  Version:          18.09.2
  API version:      1.39 (minimum version 1.12)
  Go version:       go1.10.6
  Git commit:       6247962
  Built:            Sun Feb 10 04:13:06 2019
  OS/Arch:          linux/amd64
  Experimental:     false
PS C:\Users\tatshar> docker-machine version
docker-machine.exe version 0.16.1, build cce350d7
PS C:\Users\tatshar> docker-compose version
docker-compose version 1.23.2, build 1110ad01
docker-py version: 3.6.0
CPython version: 3.6.6
OpenSSL version: OpenSSL 1.0.2o  27 Mar 2018
```

Use the following commands in the Powershell or Windows Console to create the Docker Machine:

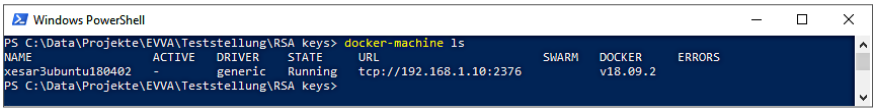
» **cd "C:\Data\Projekte\EVVA\Teststellung\RSA keys" docker-machine create --driver generic --generic-ip-address 192.168.1.10 --generic-ssh-key id_rsa --generic-ssh-user user xesar3ubuntu180402**

- Replace **C:\Data\Projekte\EVVA\Teststellung\RSA keys** with the path into which you previously copied the files with WINSCP
- **192.168.1.10** is the IP address of the Ubuntu server, which was statically assigned during the installation
- **user** is the username of the Ubuntu server that was created during the installation

- **xesar3ubuntu180402** is the name that should be given to the Docker Machine



» Using the command**docker-machine ls** check that the Docker Machine is running



» Connect the **coding station** via USB to your administrator PC

» Insert your **AdminCard** into the card slot in the coding station.

12.5 Xesar 3.2 installation

» Download the latest Xesar 3.2 software

› **https://www.evva.com/uk-en/products/electroniclockingsystem-saccesscontrolsystems/xesar/download-xesar-software/**

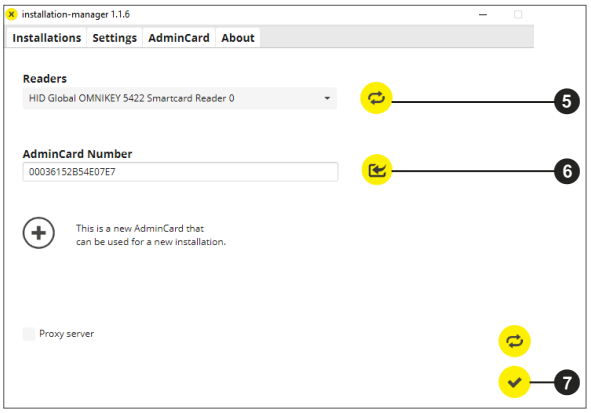
» Open the Installation Manager

» Select the tab **AdminCard**

» Load the card reader ❺

» Load the AdminCard ❻

» Confirm the entry ❼

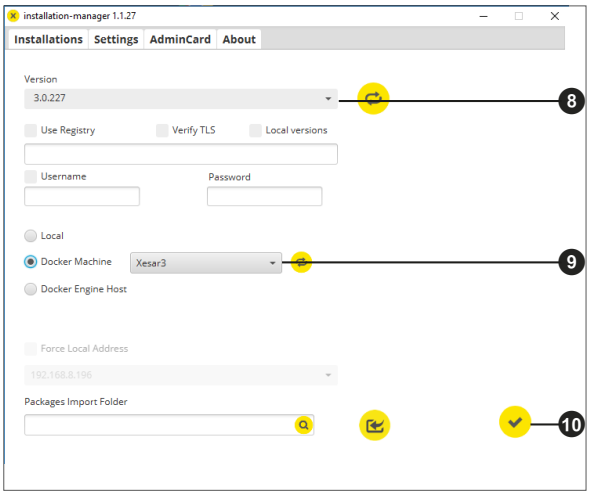


» Select the tab **Configuration**

» Select the Xesar software version❽

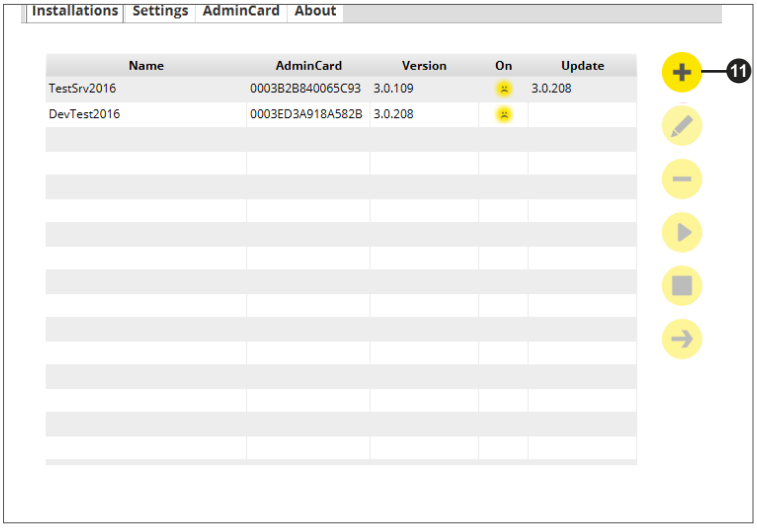
» Select the previously created Docking Machine ❾

» Confirm the entry ❿



» Select the tab **Installations**

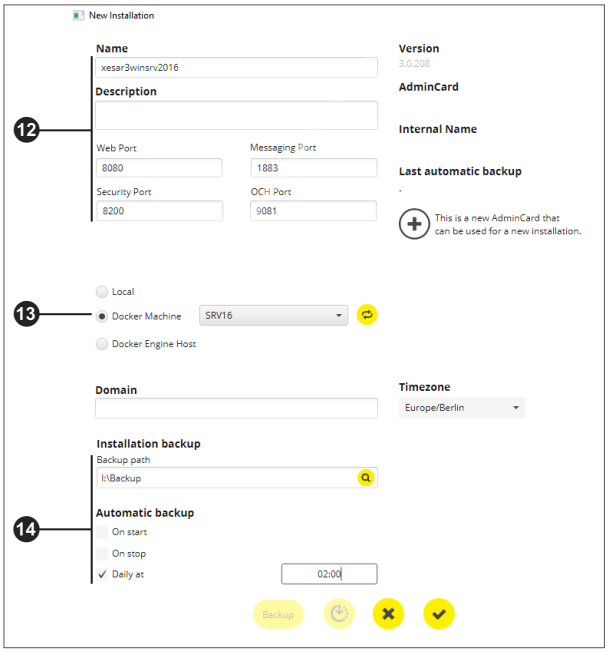
» Using the "+" button, ⓫ add a new system



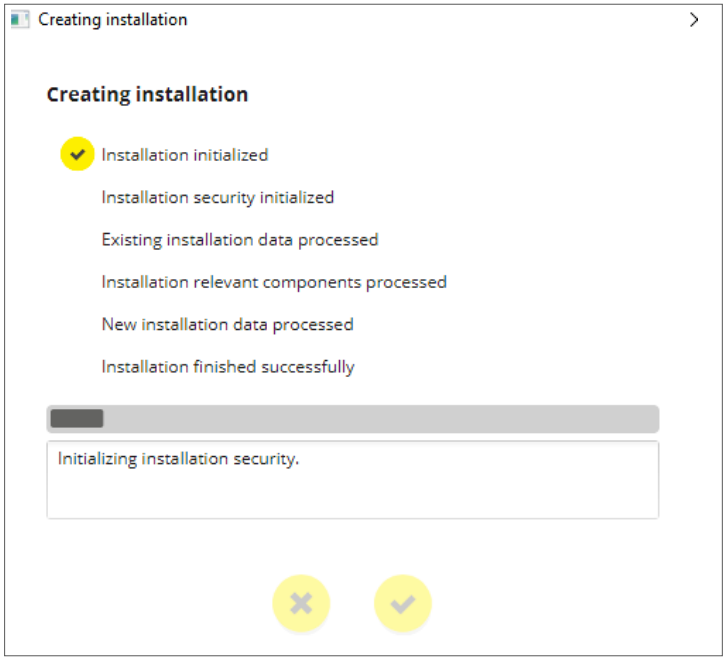
» Fill in the data ⓬

» Select the Docker Machine ⓭

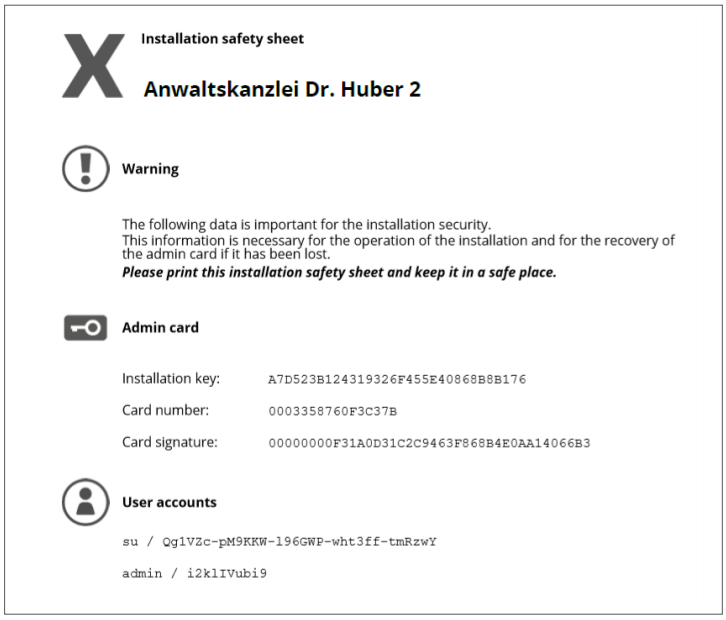
» Set up the automatic backup ⓮



The system is created (important installation information is shown).



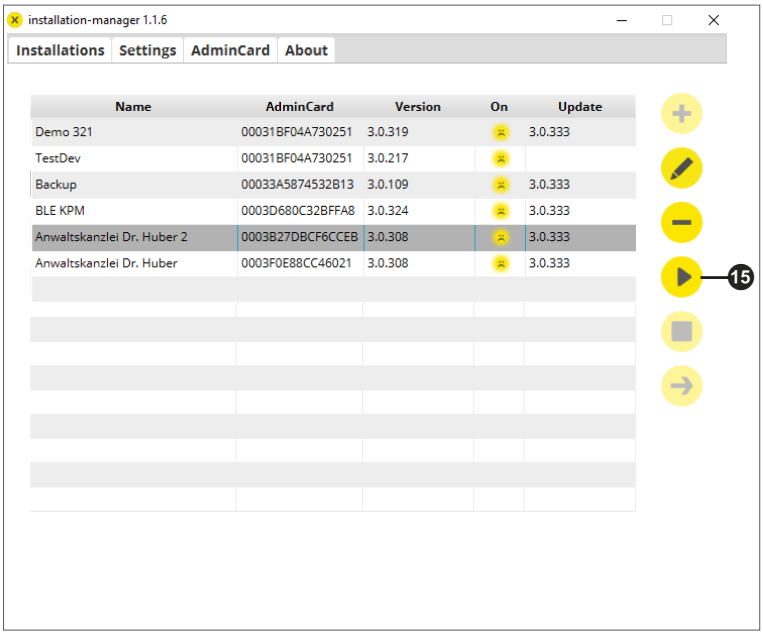
The most important system data are output in the document “Installation Information”.



Important:
Without this data, the system can not be restored in the event of a fault.
Print “Installation Information” document and keep in a safe place.

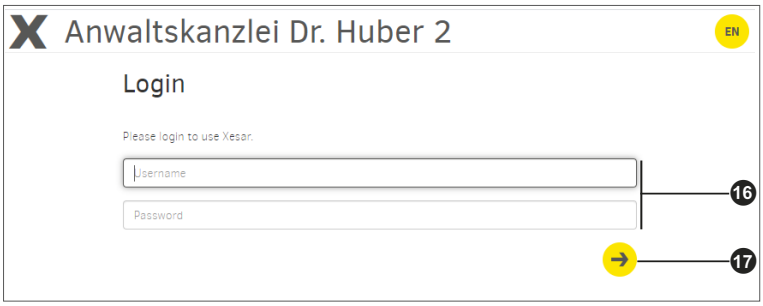
» Select the desired system

» Start by clicking on the arrow ⓯



» Log in with the login details you received in the "Installation Information" document (admin / password) ⓰

» Click on the arrow ⓱



You will now be taken to the Xesar 3.2 dashboard and can operate the system.

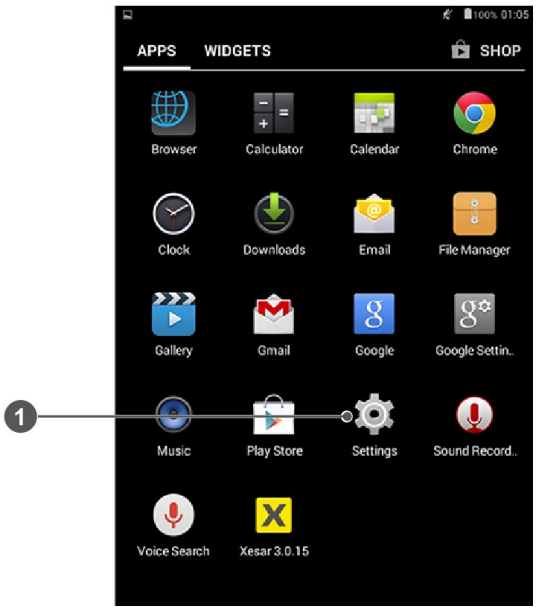
13 Manually uninstalling and installing the Xesar maintenance app

(Upgrade from Xesar 2.2 or 3.0 to Xesar 3.2)

When upgrading from Xesar 2.2 or 3.0 to Xesar 3.2, the old maintenance app must be manually uninstalled on the tablet and the new Xesar 3.2 maintenance app must be installed manually.

» Start your tablet and proceed as follows:

» **1. Step:**
Click on Settings ❶ in the main menu

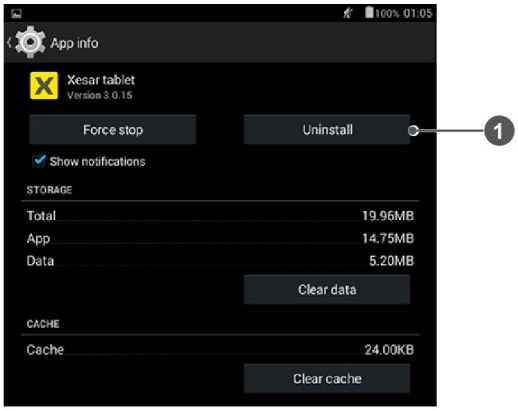


2. Step

Click on Apps ❶.

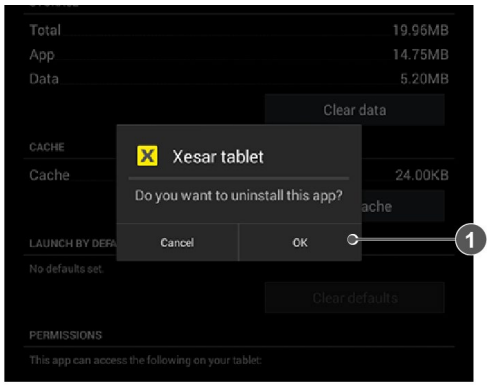
3. Step:

Uninstall ❶ the Xesar maintenance app.

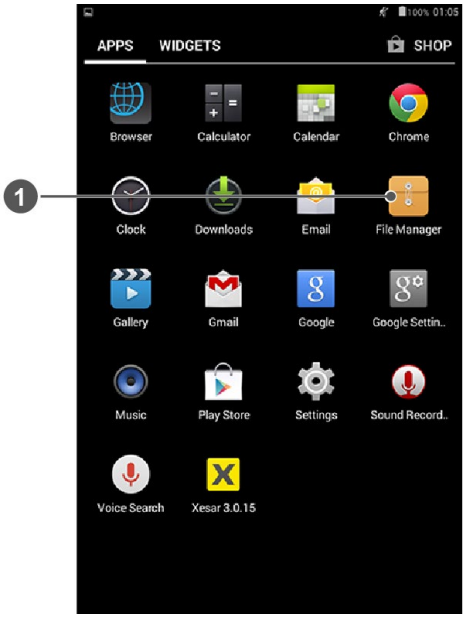


4. Step:

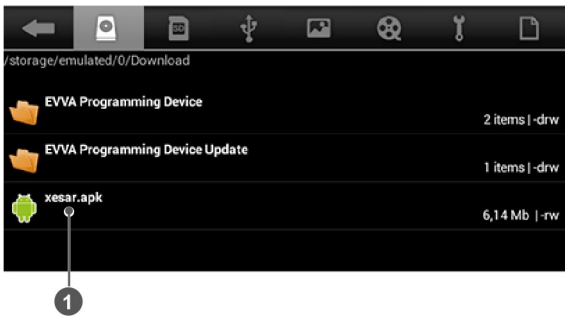
Click OK ❶.



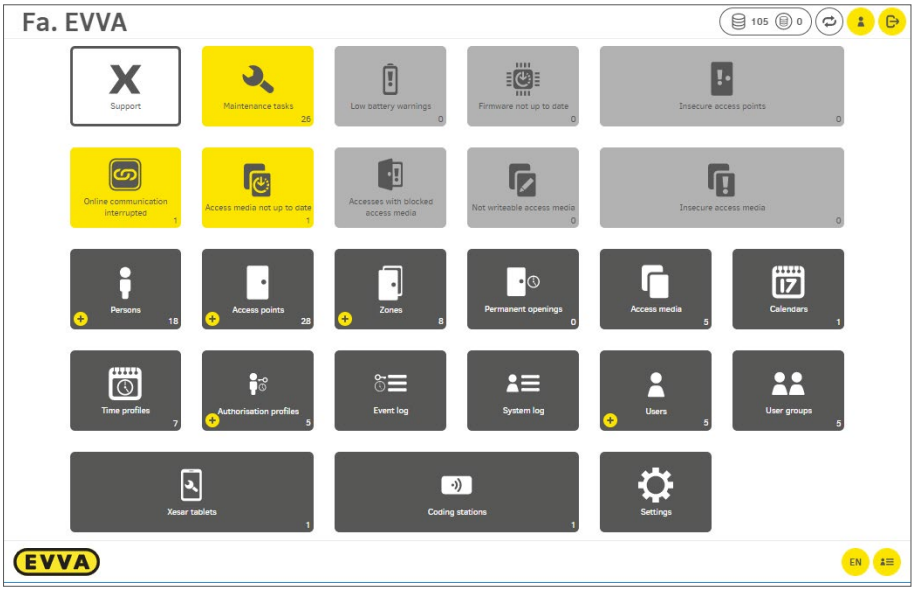
» **5. Step:**
Open the file manager on your Xesar tablet ❶.



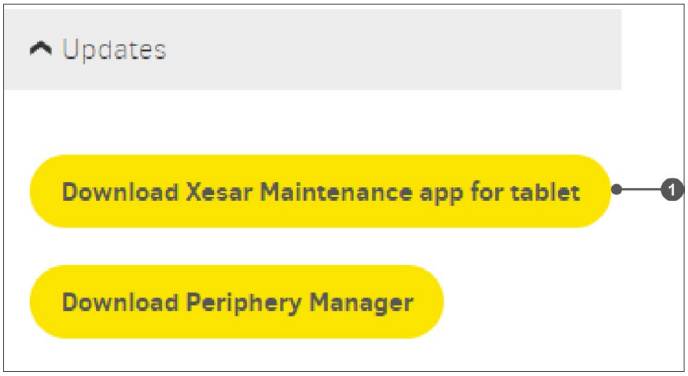
» **6. Step:**
Click on the Download folder and delete the .apk file ❶.



» **7. Step:**
Click the support tile in the Xesar dashboard **Support**.



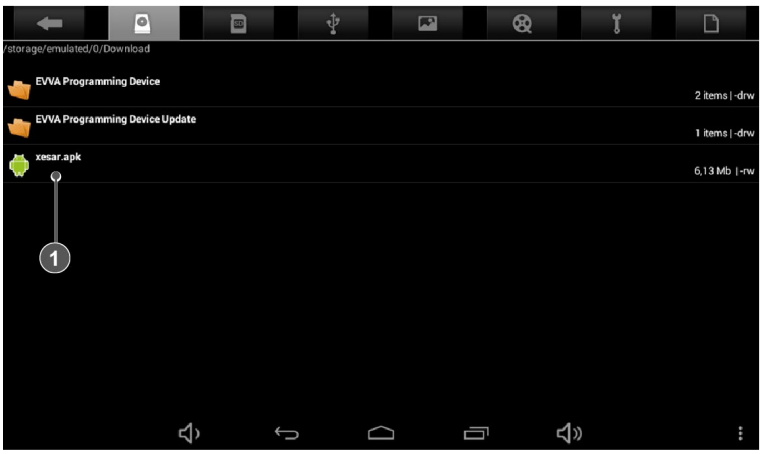
» **8. Step:**
Download Xesar tablet:
Download the current Xesar maintenance app under **Updates**.
Click on **download Xesar maintenance app for tablet ❶**.



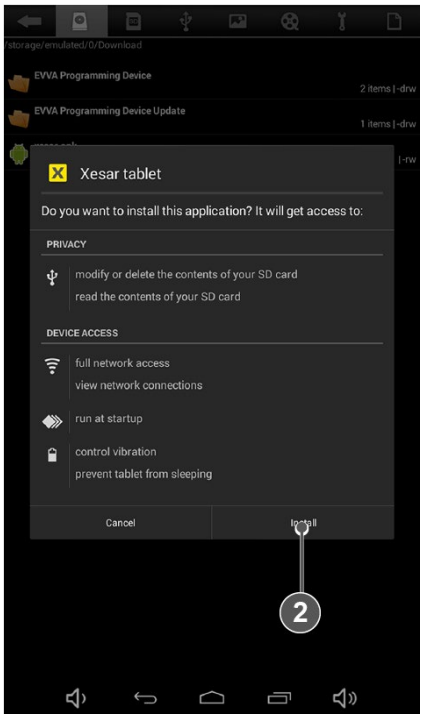
» **9. Step:**
Connect the Xesar tablet to the USB port of your computer and use the mouse to drag the file into your tablet's file manager.

» **10. Step:**

Click the .apk file ❶ to install the Xesar app on your Xesar tablet.



Click on Install ❷.



» **11. Step:**

Launch the Xesar maintenance app and connect the tablet to the Xesar software. See chapter "Connecting the tablet to the Xesar software".

14 Creating Xesar systems on a PC

14.1 Installation requirements

A computer with Windows 10 Pro, Enterprise or Education is required to create Xesar systems on a PC. Hyper-V is already integrated in these versions of Windows.

14.2 Hyper-V

› **https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v**

Hyper-V is detected and activated when the Installation Manager is started.

Hyper-V is integrated into Windows as an optional feature. A Hyper-V download is not available.

» Review the requirements:

- Windows 10 Enterprise, Pro or Education
- 64-bit processor with SLAT (second level address translation)
- CPU support for VM Monitor Mode Extension (VT-c on Intel CPUs)
- At least 8 GB RAM, of which 4 GB is needed for installing the system

The Hyper-V feature cannot be installed on Windows 10 Home.

For more information and troubleshooting, see

› **https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/hyper-v-requirements**

14.3 Programmes for creating and managing Xesar systems

The following programs are required to create and manage Xesar systems:

14.3.1 Installation manager

You can manage one or more systems with the Installation Manager. In addition, Xesar system settings can be configured.

The following tasks can be performed:

- Easy creation of Xesar systems on PC or server
- Starting and Stopping a system
- Admin Card management
- Performing updates
- Management of multiple systems.
- Add KeyCredits and KeyCredit Xesar Lifetime
- Setting the system backup options
- Replacement of defective Admin Cards
- Setting of system ports

14.3.2 Periphery Manager

For single-user systems, the coding station is managed in the Installation Manager. An additional installation of the Periphery Manager is not necessary.

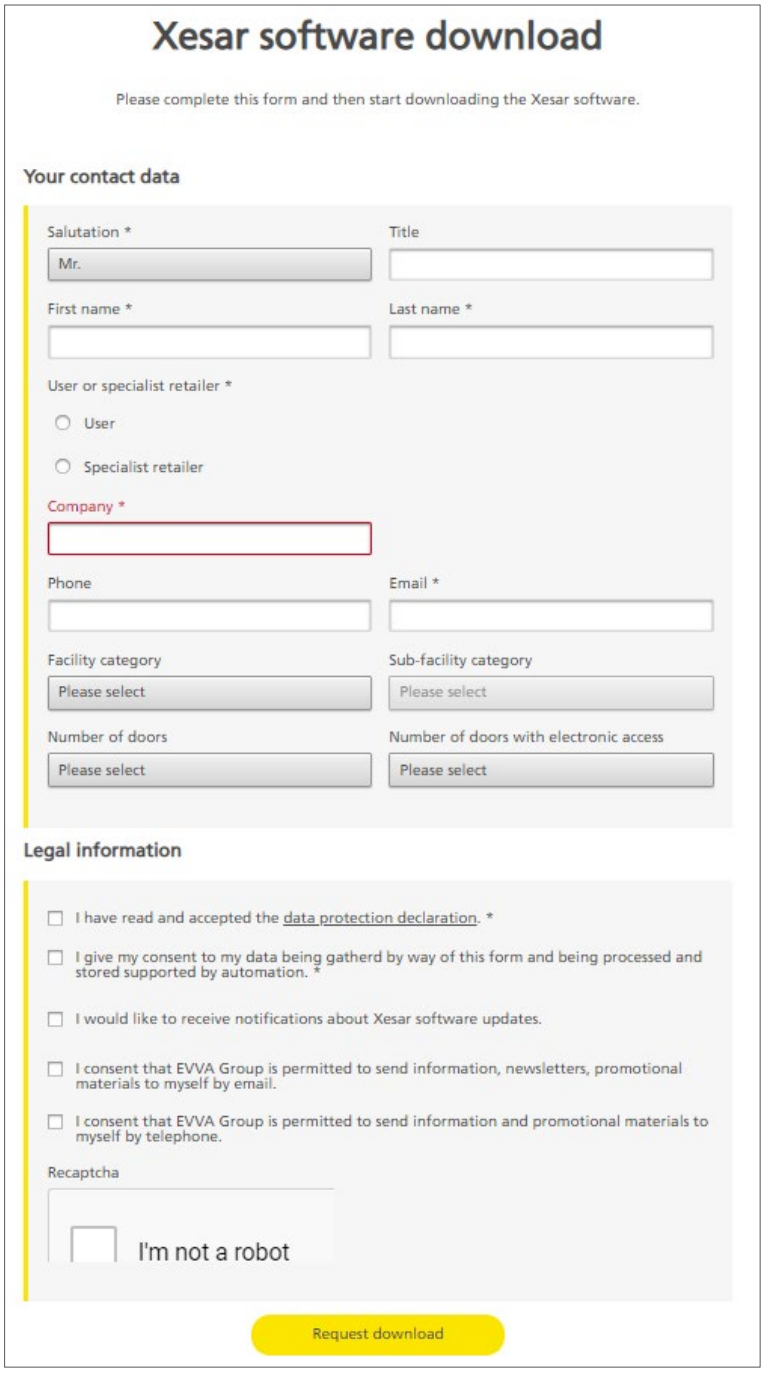
The Peripheral Manager permits the operation of a coding station on an administrator PC and on the client PCs in a multi-user system.

The Periphery Manager can be downloaded from the **Xesar software > Support > Updates**.

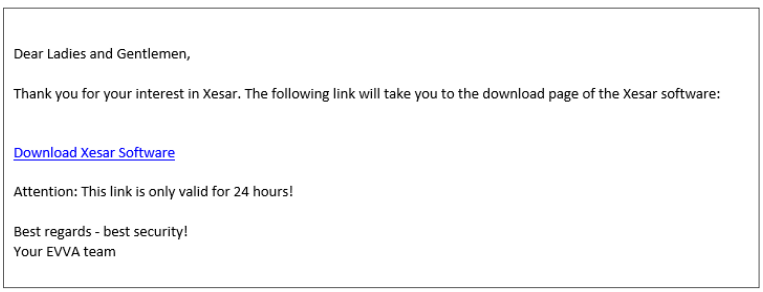
14.3.3 Xesar software

The Xesar software is an application that is started from the installation manager and runs in a browser. The Xesar software can be used to manage a system started in the Installation Manager on the dashboard.

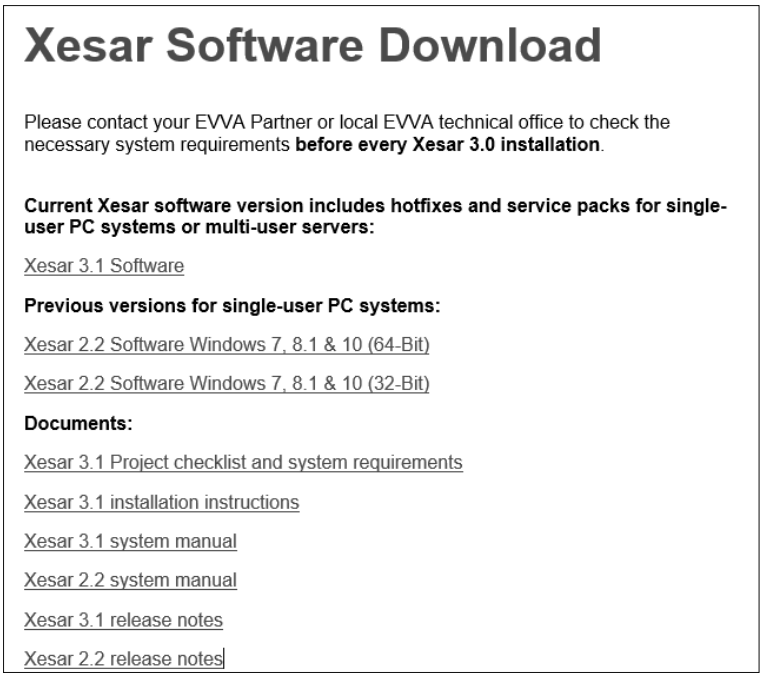
You can download the current installation manager from the EVVA website by clicking on the Software tab.



» Complete and submit the "Download Xesar software" form.



You will receive an email with a temporary download link to the email address you provided in the “Download Xesar Software” form.



Xesar Software Download

Please contact your EVVA Partner or local EVVA technical office to check the necessary system requirements **before every Xesar 3.0 installation**.

Current Xesar software version includes hotfixes and service packs for single-user PC systems or multi-user servers:

Xesar 3.1 Software

Previous versions for single-user PC systems:

Xesar 2.2 Software Windows 7, 8.1 & 10 (64-Bit)

Xesar 2.2 Software Windows 7, 8.1 & 10 (32-Bit)

Documents:

Xesar 3.1 Project checklist and system requirements

Xesar 3.1 installation instructions

Xesar 3.1 system manual

Xesar 2.2 system manual

Xesar 3.1 release notes

Xesar 2.2 release notes

» Download the current Installation Manager.
» Start the *.msi file.

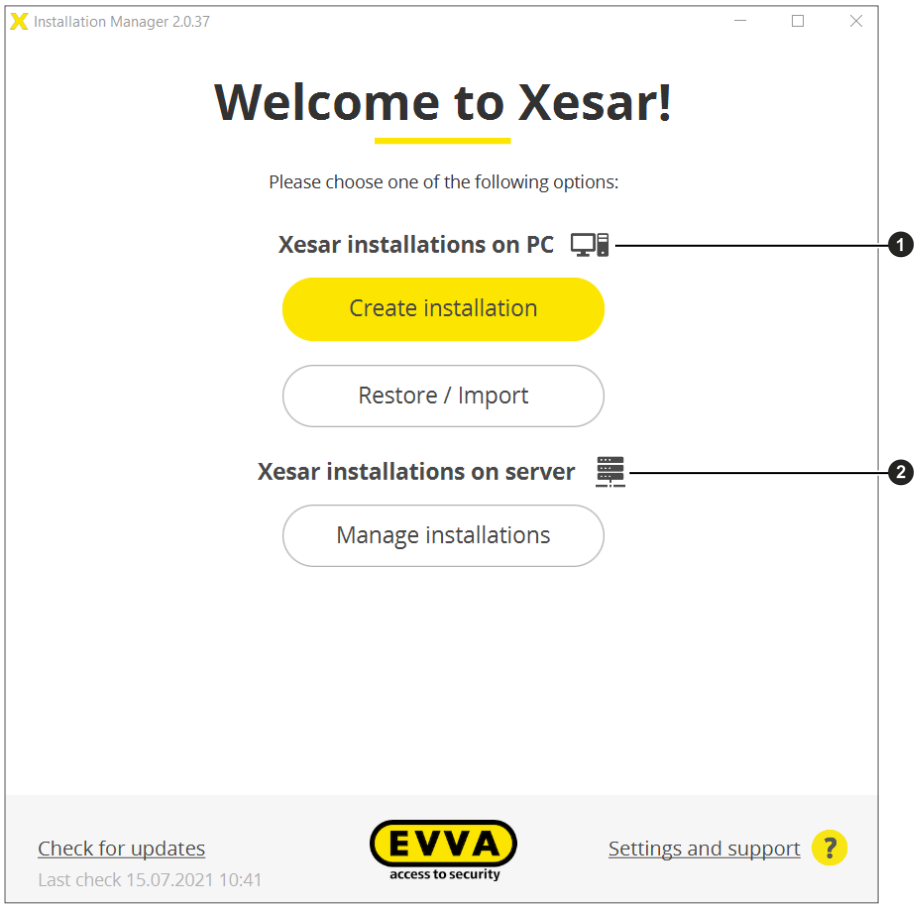
The installation manager is installed automatically and a program shortcut is created in the start menu and on the desktop.

» Start the installation manager by clicking on one of the links.

14.4 Start installation manager

» Start the installation manager by clicking on one of the links.

The start window "Welcome to Xesar!" contains a grouping in "Xesar systems on PC" ❶ and "Xesar systems on server" ❷.

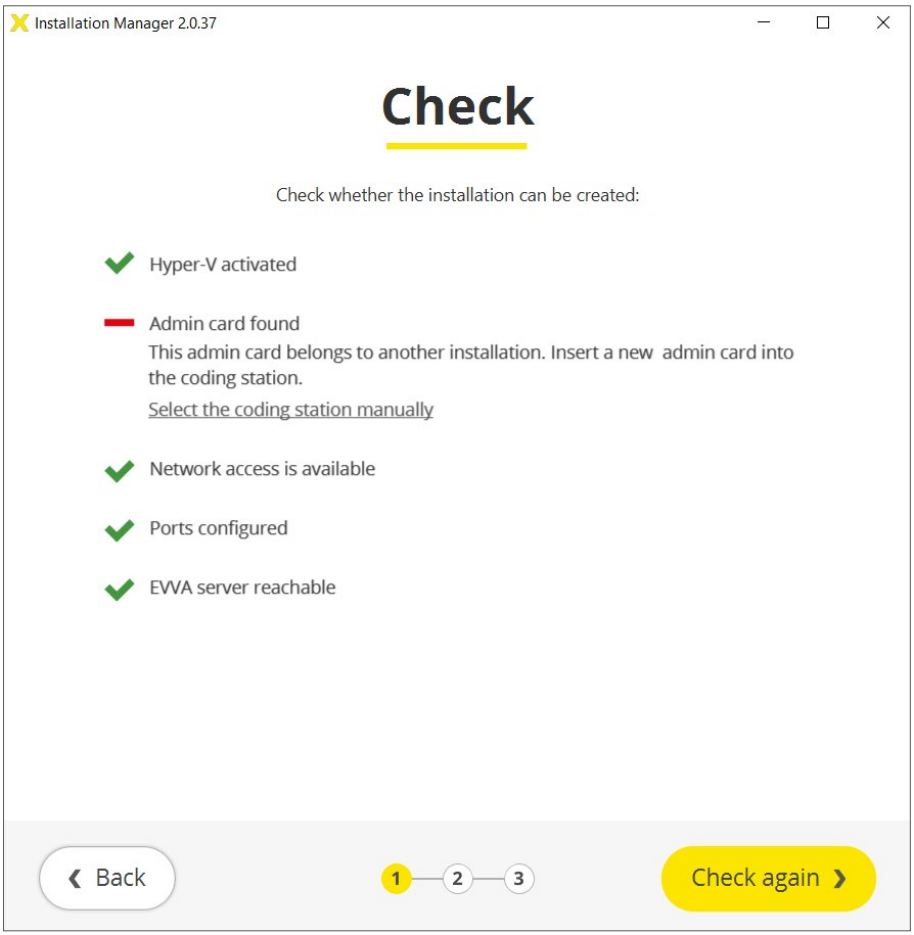


14.4.1 Creating a Xesar system on a PC

» Click the button **Create system** to create a new Xesar system on a PC.

You will now be guided step by step through the creation process.

» **1. Step:**
Check the requirements of the PC.



Please refer to the chapter “System requirements” or the project checklist for the necessary system requirements.

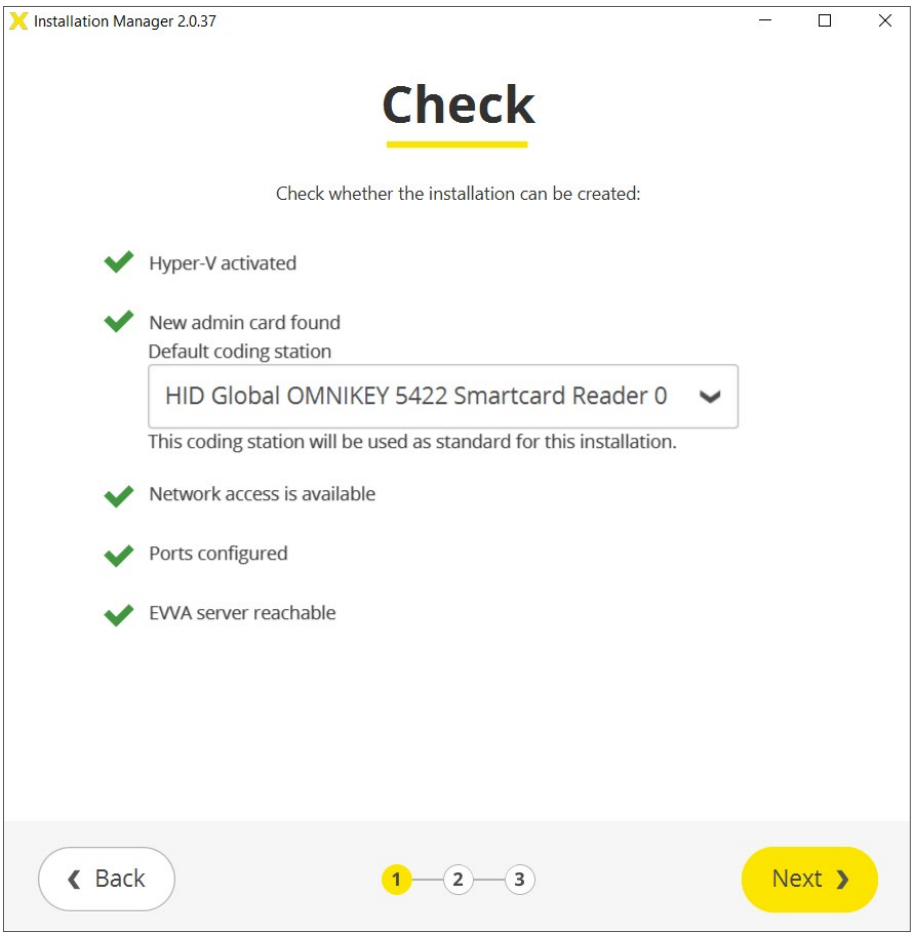
The following requirements are automatically checked:

- Hyper-V is installed and enabled on the PC.
- A coding station is connected and a new and valid Admin Card is inserted.
- The network authorisation checks whether the Installation Manager has been installed on a physical data carrier and not on a network drive.
- The ports required by Xesar are both free and available.
- The EVVA server can be accessed via the Internet. This is necessary, for example, to check the list of available updates.

If all the requirements necessary for installation are not met, error messages with suggested remedies are displayed.

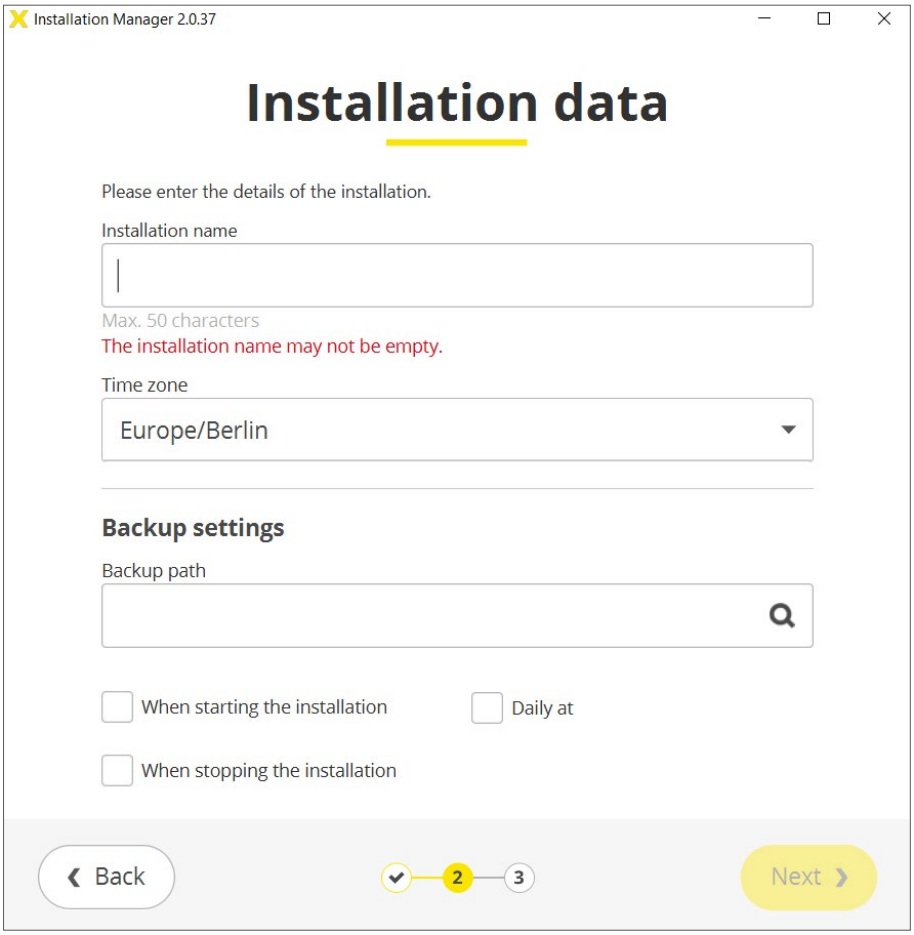
» Try to remedy the problem according to the suggestion click **Check again**.

If the problem cannot be remedied, please contact your EVVA partner or the EVVA technical office.

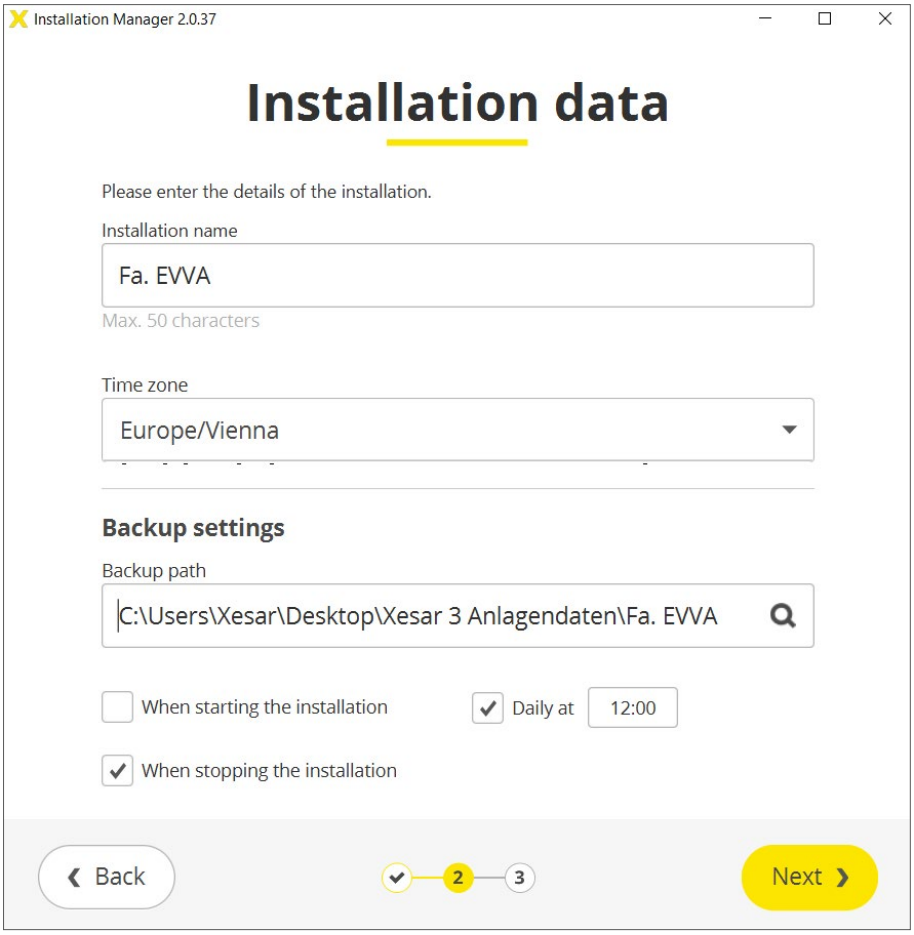


When all requirements have been successfully verified, click **Next** to continue the process.

» **2. Step:**
Insert the installation data and the desired backup settings in the fields provided.

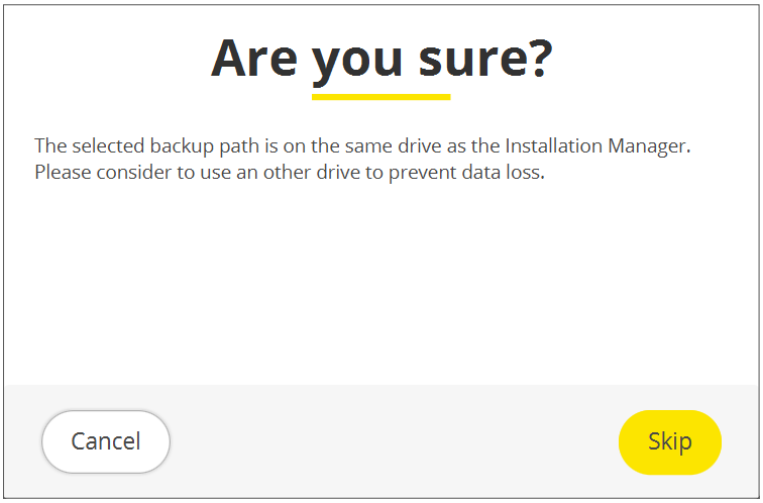


Several backup options can be selected.



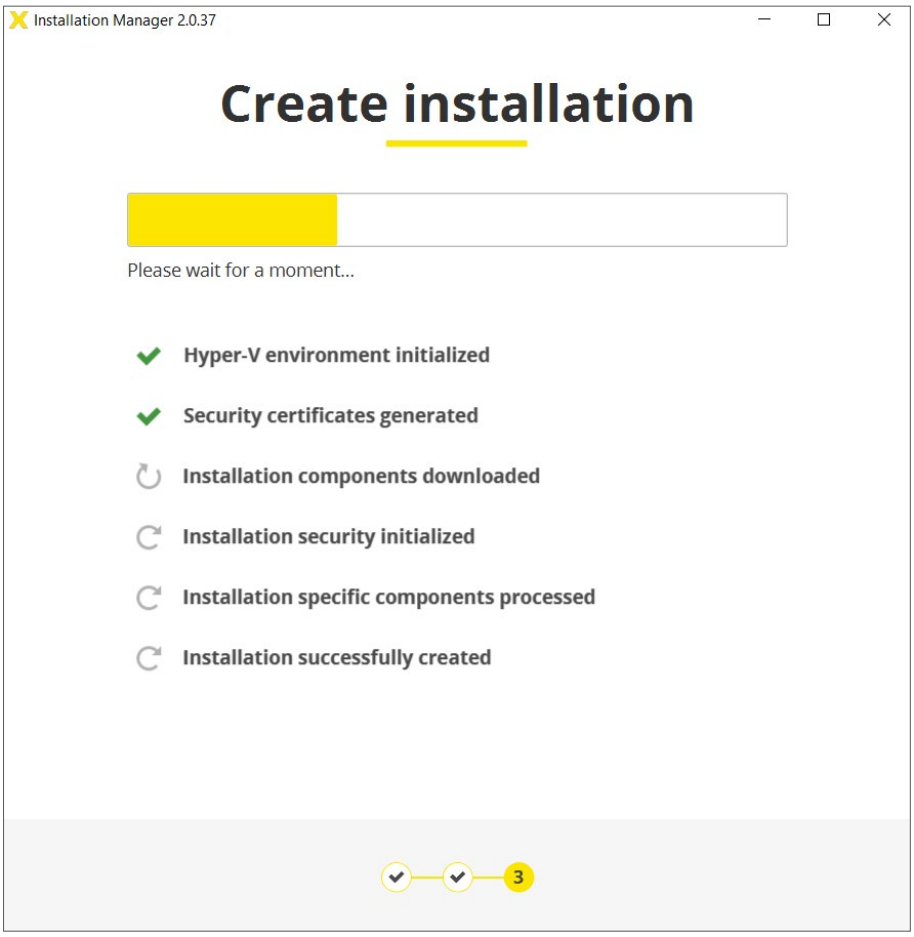
In order to prevent data loss in the event of a hardware problem, backup data should not be saved on shared Xesar software drives.

If you select the backup path on the installation manager drive, the message "Are you sure?" appears.

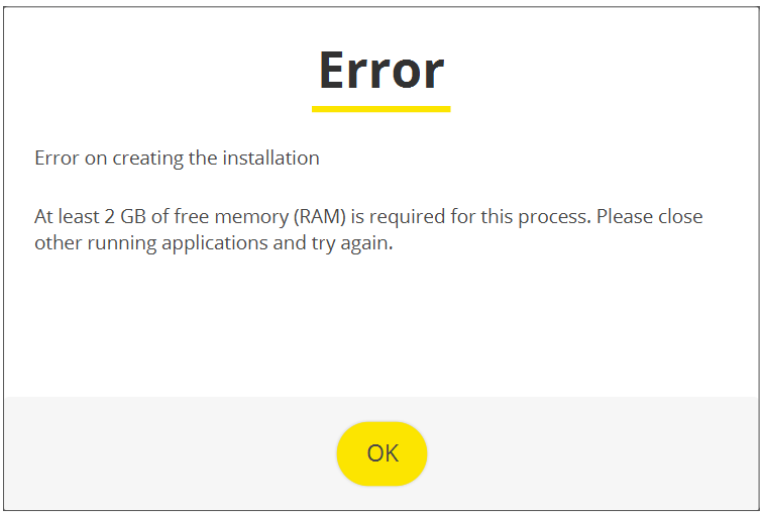


Click **Cancel,** to return and then specify a new backup path. Click **Skip** to ignore the warning.

» **3. Step:**
Create system



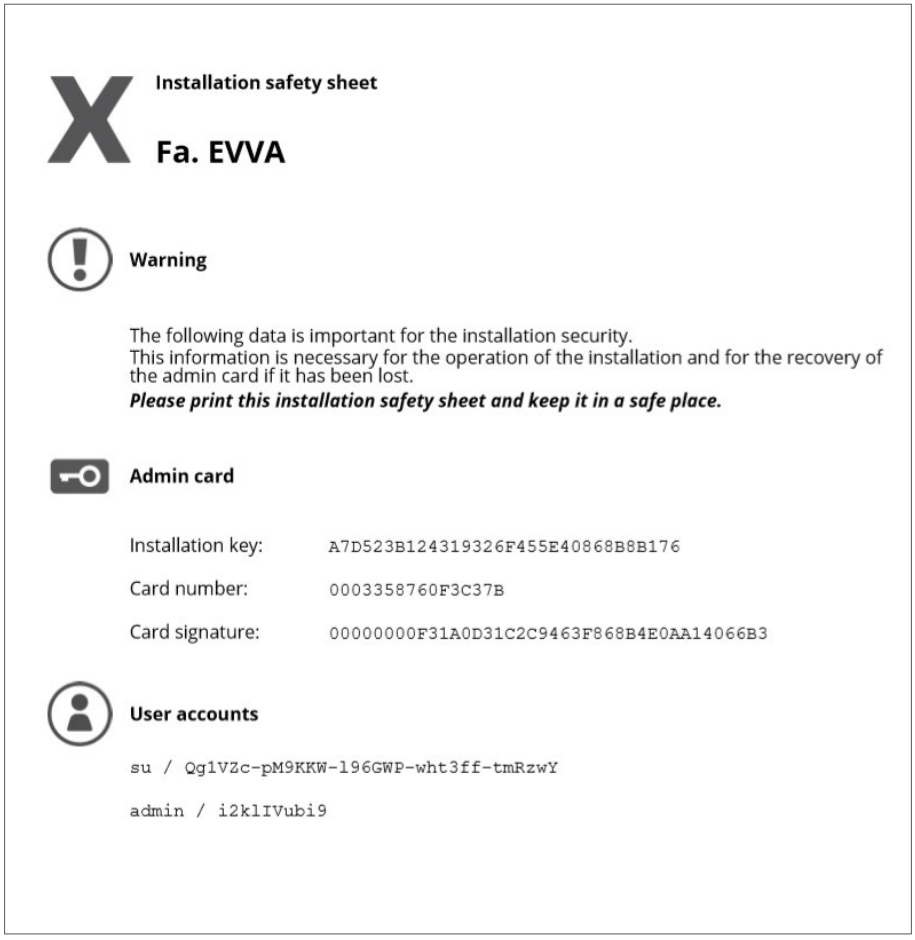
The following error message appears if there is too little memory available during the installation process (at least 2 GB).



14.4.2 System Safety Sheet

After successful installation of the system, the system safety sheet with important system information is generated and automatically displayed as a PDF.

This contains the user passwords for logging in as system administrator (su) and administrator (admin).



Installation safety sheet

Fa. EVVA

Warning

The following data is important for the installation security.
This information is necessary for the operation of the installation and for the recovery of the admin card if it has been lost.
Please print this installation safety sheet and keep it in a safe place.

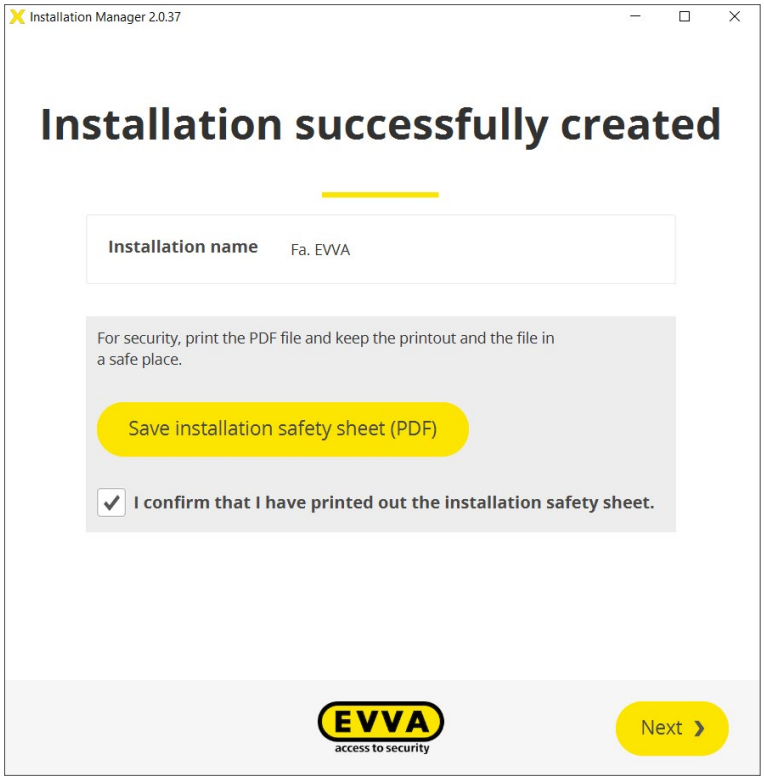
Admin card

Installation key:	A7D523B124319326F455E40868B8B176
Card number:	0003358760F3C37B
Card signature:	00000000F31A0D31C2C9463F868B4E0AA14066B3

User accounts

su / Qg1VZc-pM9KKW-l96GWP-wht3ff-tmRzwY

admin / i2klIVubi9



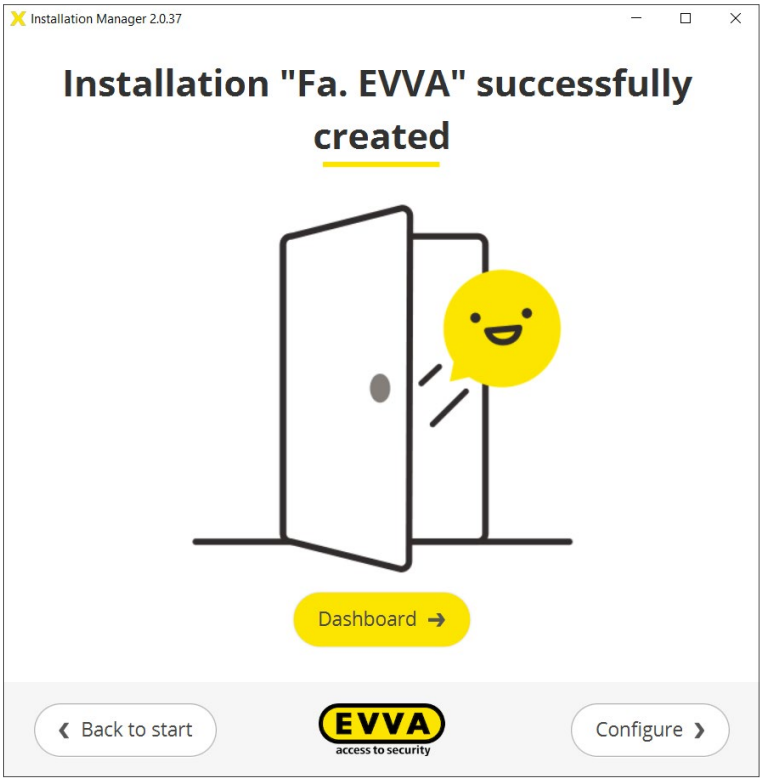
You can also open the system safety sheet by clicking on the button **Open system safety sheet (PDF)**.

Print the system safety sheet. Confirm the printout by clicking here and keep the printout in a safe place.

If the Admin Card is lost or defective, the information in the system safety sheet is the only way to continue operating the system.

EVVA cannot restore the data if the system safety sheet including the system information is missing!

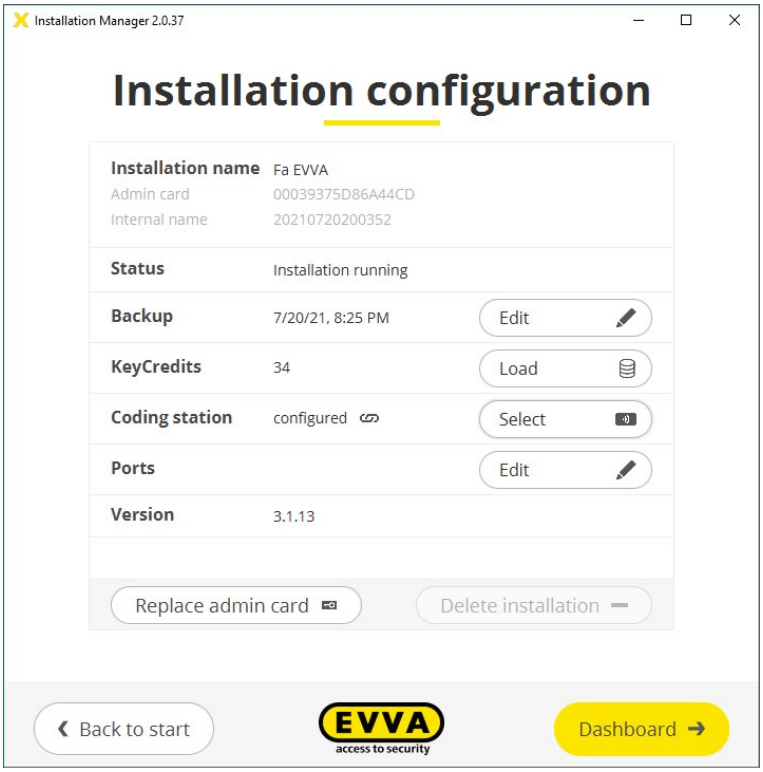
» Click **Next** to begin the installation.
(It may take a few minutes for the system to start).



- Click on the button **Dashboard** - you will be taken to the system management login

- Click on the button **Configure** - you will be taken to the system configuration page.

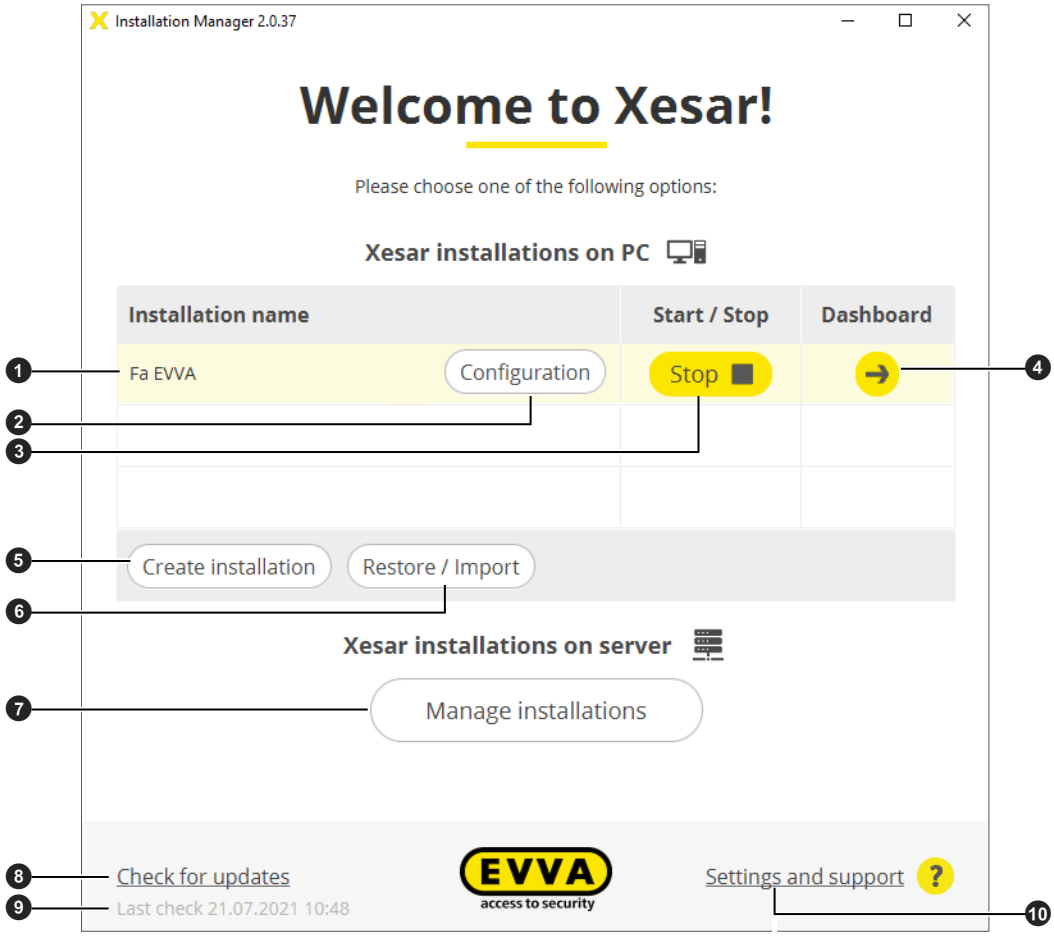
Here you can see an overview of all important system settings.
If necessary, system-relevant changes can be made.



This completes the installation of the system.

» Click the button **Return to start** – you will be taken to the Installation Manager start page.

15 Start Page Installation Manager

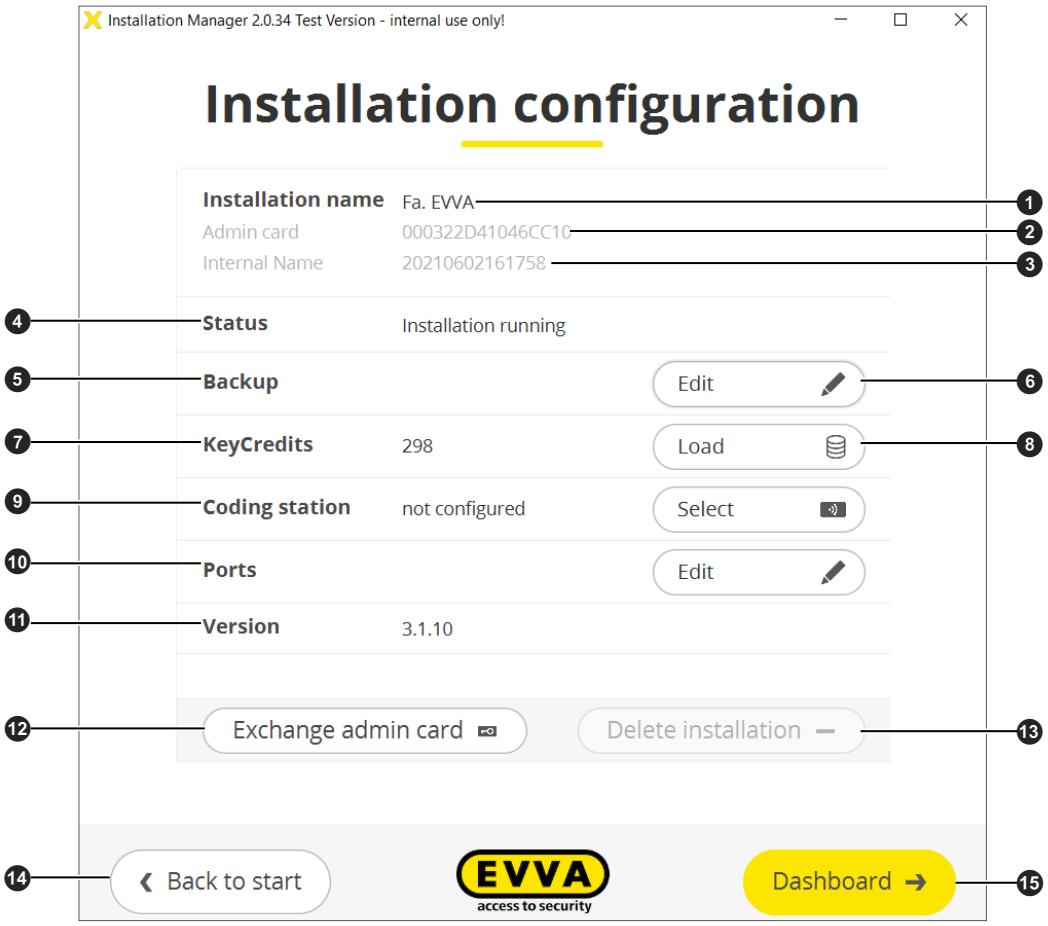


Features of the Installation Manager start page:

- Display of the Installation Manager version
- PC systems:
  - System name ❶
  - Button **Configuration** ❷ to go to the system configuration page.
  - Button **Start/Stop** ❸ to start or stop the selected system.
  - Button **Dashboard** ❹ for system login page
  - Button **Create system** ❺ to start the installation process for a new system.
  - Button **Restore/Import** ❻: System recovery using a backup file or upgrade of an existing Xesar 2.2 system.
- Xesar systems on server:
  - Button to view Xesar systems on server and Xesar 3.0 systems after update to 3.2 (see chapter "Xesar systems on server") ❼.
- Button **Check Update**: Check for updates to the Installation Manager and Xesar software. If an update is available, it is displayed ❽.
  Clicking on the button takes you to the update page.
  - Check date of last update ❾.

- Settings and support ❿ (only for PC systems):
  - Autostart: Automatic start of the installation manager after booting the PC can be activated or deactivated.
  - Proxy settings: If necessary, proxy settings can be configured here.
  - Support information: Generation of a data file for improved fault analysis by EVVA support in the event of a fault.

15.1 Configuration of the system

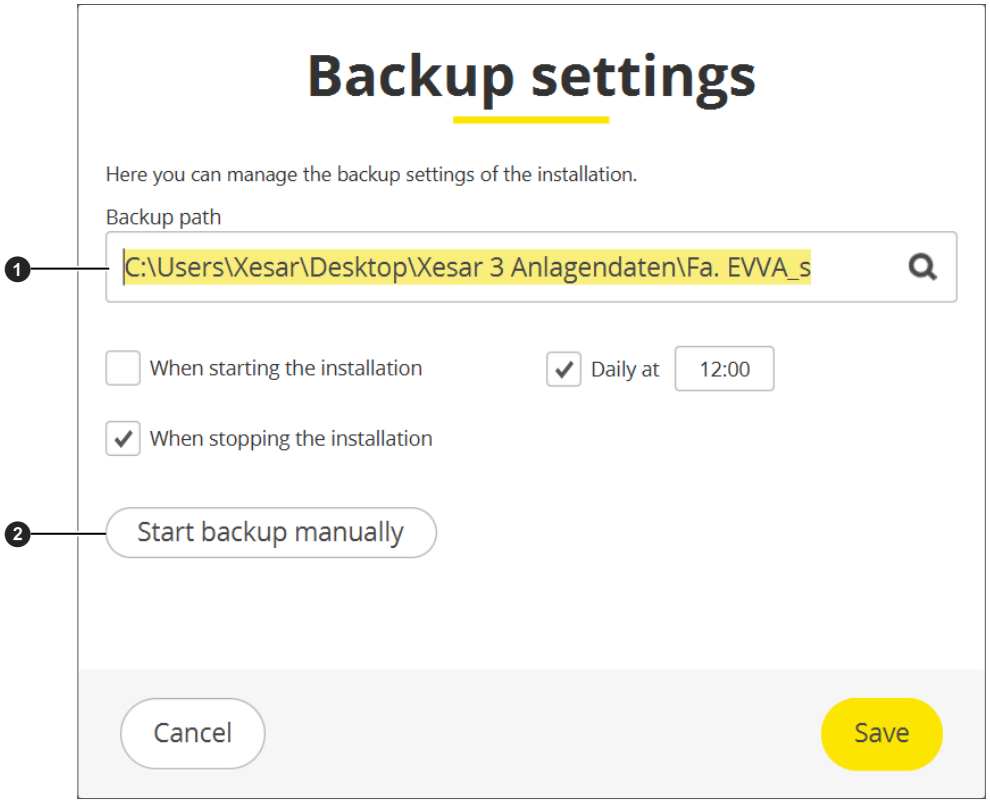


System configuration page functions:

- System name ❶
- Admin Card ❷: Admin Card number
- Internal number of system ❸
- Status of system ❹:
  - System is running
  - System stopped

- Backup ❺:
  - Date of last backup
  - Button **Setting** ❻ to set the time of the system backup.
- KeyCredits ❼:
  - Number of available KeyCredits or view of Lifetime icon∞.
  - Button **Add** ❽ to load KeyCredits.
- Coding station ❾: Selection of coding station for access media management
- Ports ❿: Port setting when standard ports are assigned (only possible when the system is stopped).
- Xesar software version ⓫
  - Button **Replace Admin Card** ⓬: Replacement in the event of a defective Admin Card.
  - Button **Delete system** ⓭: Delete a Xesar system on a PC (only possible when the system is stopped).
  - Button **Return to start** ⓮: Return to the Installation Manager start page.
  - Button **Dashboard** ⓯: To register the system in the browser.

15.1.1 Backup settings



- Backup path: ❶:
  - Enter the desired path for the backups of your system.

The drive should not be identical to the system drive.

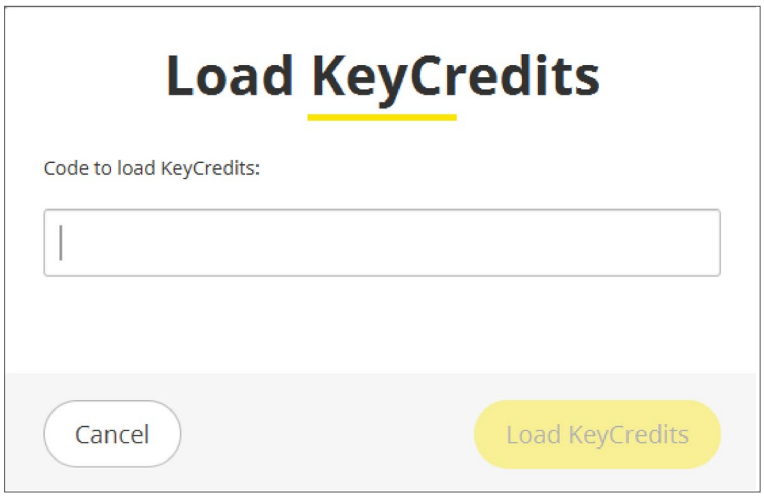
- Setting option for automatic backups:
  - Backup when starting the system.
  - Backup when stopping the system (recommended).
  - Backup – daily at a defined time.
- Button **Start a manual backup** ❷: A manual backup is possible at any time.

The backup files can be found under the specified backup path.

15.1.2 Adding KeyCredits

KeyCredits are charged when access authorisations for access media are created and changed.

Two licence models are available for managing systems:
- Xesar unit-based KeyCredits
- Xesar lifetime-based KeyCredits



» Enter the code to add KeyCredits in the input field and click **Add KeyCredits**.

If KeyCredits are added, the credit balance on the configuration page in the installation manager or on the dashboard of the installation increases by the corresponding value. The KeyCredits used for authorisation creation and changes are deducted from this credit balance.

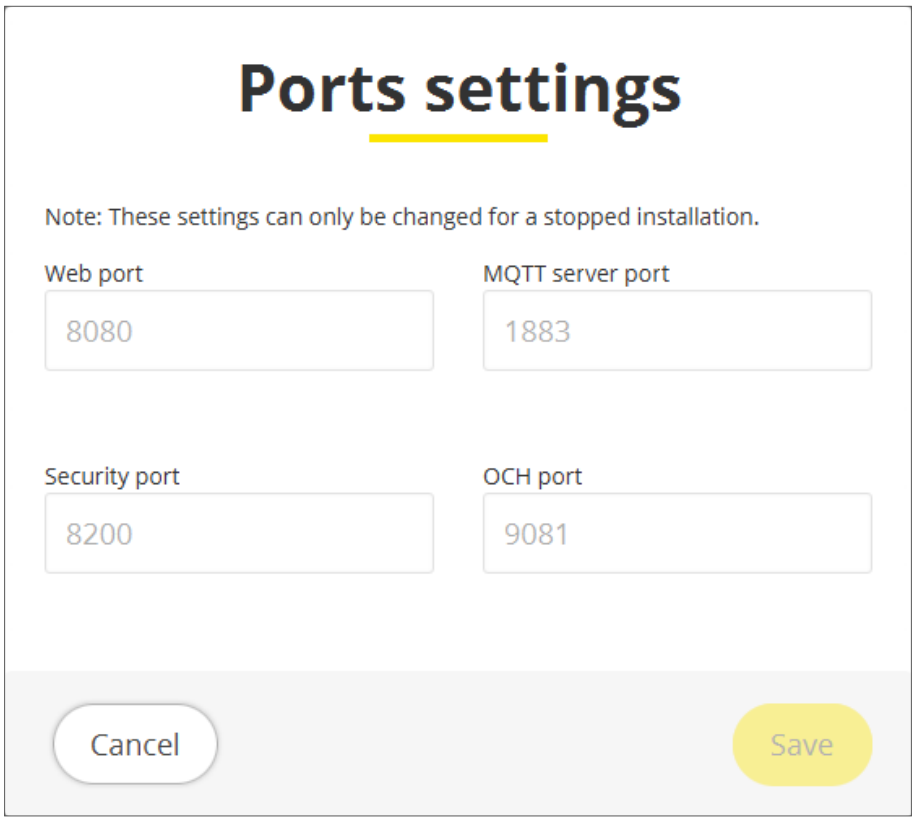
The Lifetime symbol is displayed for KeyCredits Xesar Lifetime. No further KeyCredits are required for authorisation creation and changes.

To add KeyCredits, the system must be started and connected to the EVVA server via the Internet.

15.1.3 Ports settings (manual setup)

The standard ports required for Xesar are automatically set up when the system is created. If these ports are not available in the system network, the ports can be entered here manually.

The system must be stopped to set up the ports manually.

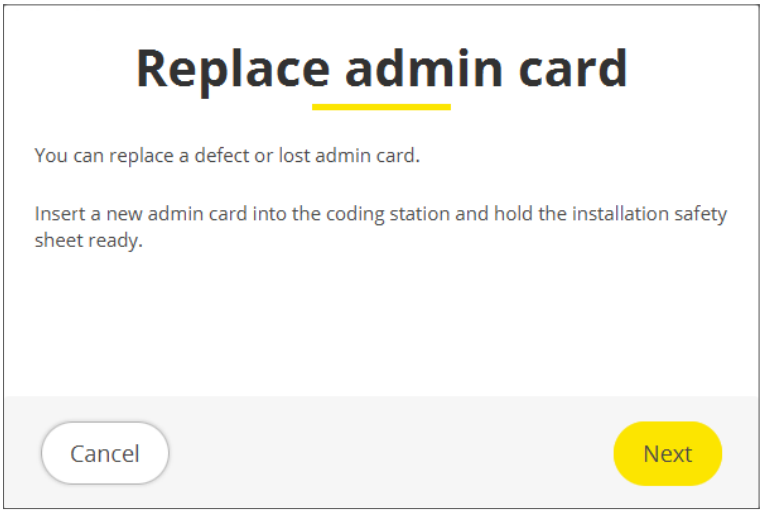


» Enter the port addresses in the input fields and click **Save**.

15.1.4 Replace Admin Card

If the system's Admin Card is defective or lost, it can be replaced with a new Admin Card.

» To do this, click **Replace Admin Card** in the configuration page and follow the instructions.



15.1.5 Delete system

» To delete a system, click **Delete**.

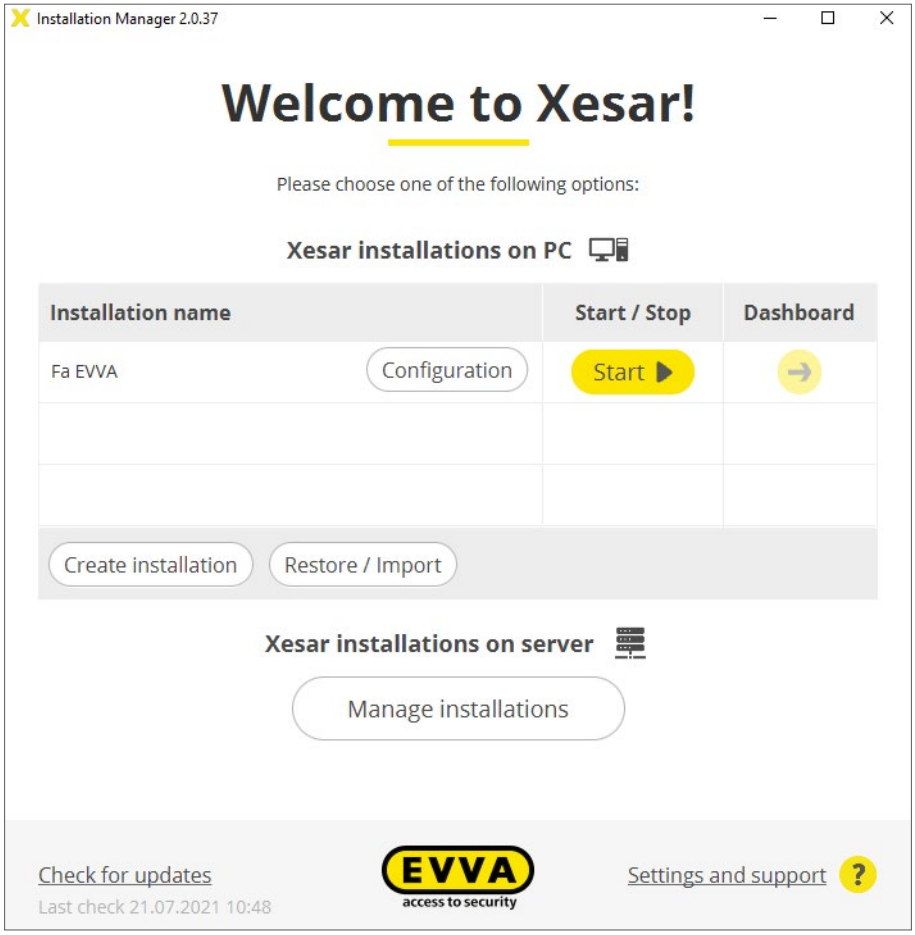
Before deleting, the system must be stopped.

15.2 Starting an existing system

» Start the Installation Manager by clicking the icon on the desktop.

The installation manager performs an automatic system check to ensure that all the necessary requirements for starting the system are met.

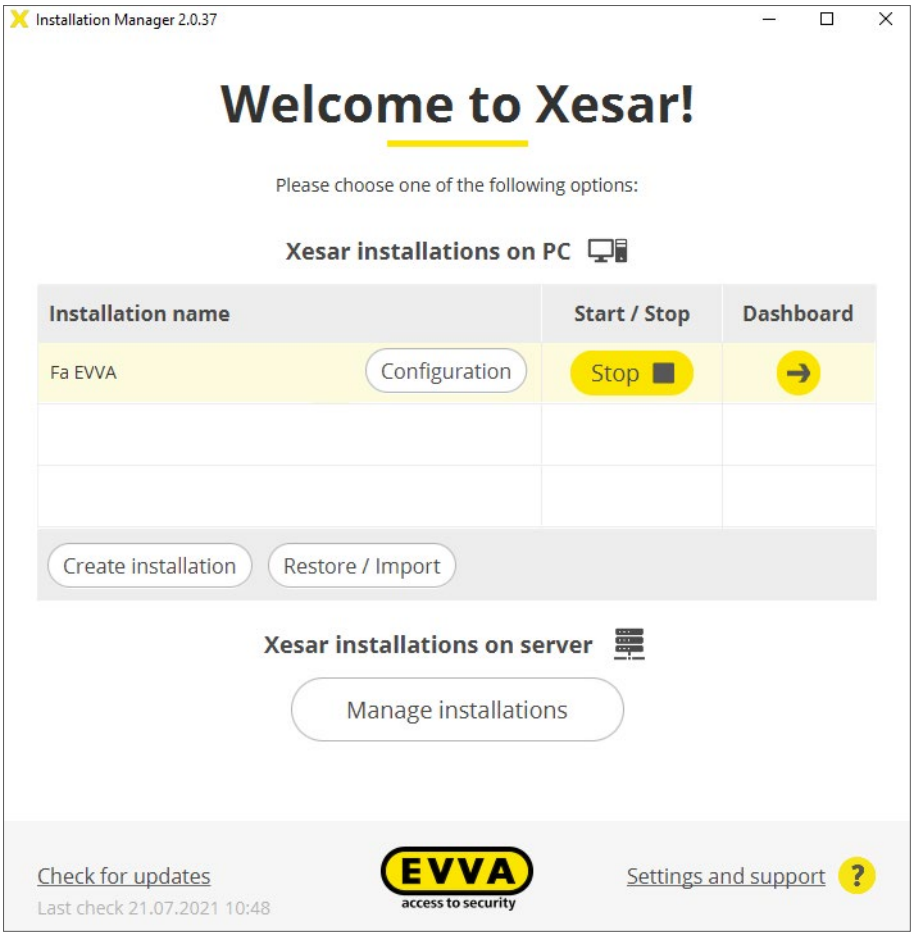
15.2.1 Starting the system with the Admin Card inserted



» Start the system by clicking on the Start button.

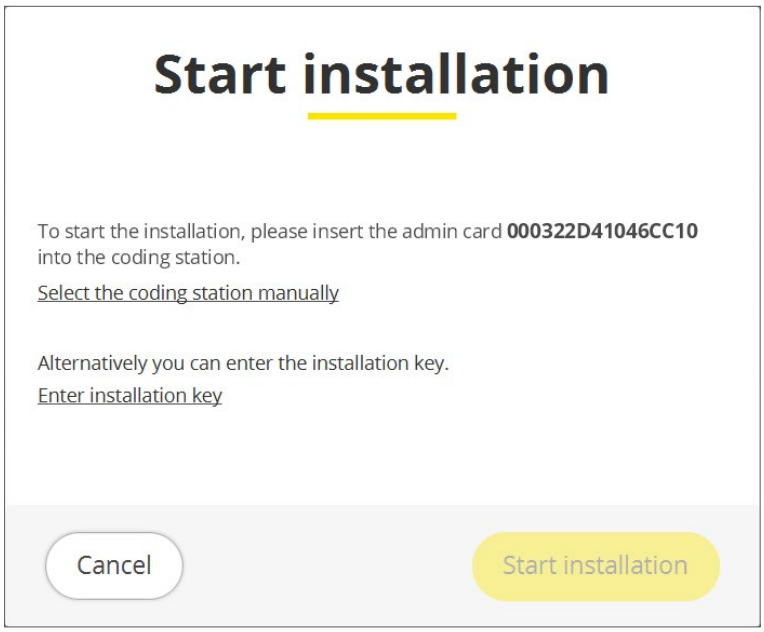
The Admin Card is then checked. If the correct Admin Card is inserted, the system is started.

» After a successful system start, press the button **Dashboard** to access the system management login.



15.2.2 Starting the system without Admin Card

If no Admin Card or the wrong one for the system is inserted, the following error message is displayed:



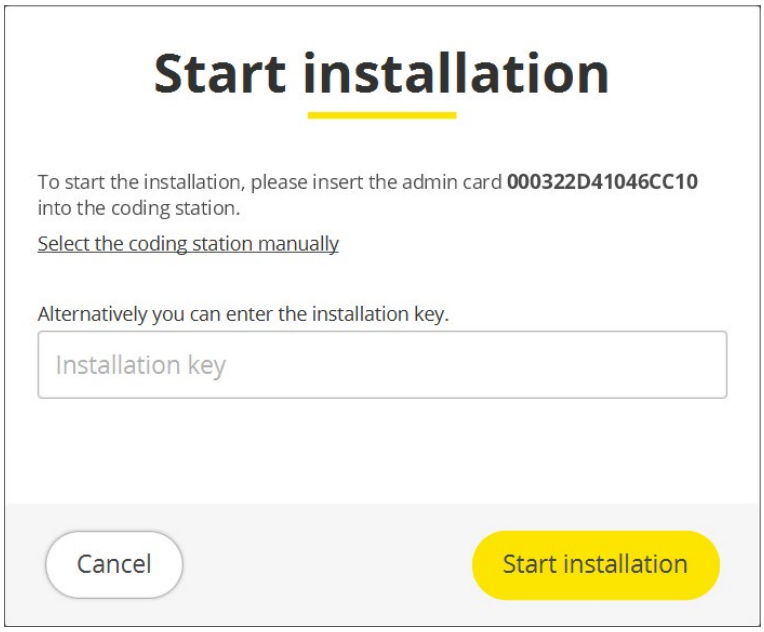
- Insert the correct Admin Card with the corresponding Admin Card number into the coding station and
- start the system.

Or alternatively:

- Enter the system key and
- start the system.

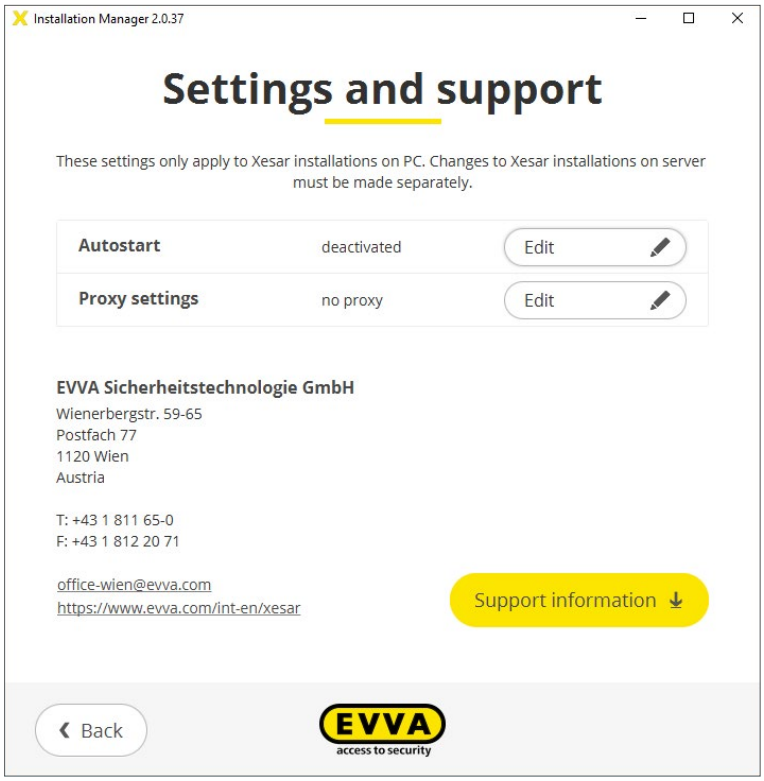
The system key can be found on the system safety sheet.

The system can only be started with the system key.
changes to the system's configuration page can only be made with the Admin Card inserted.



15.3 Settings and support

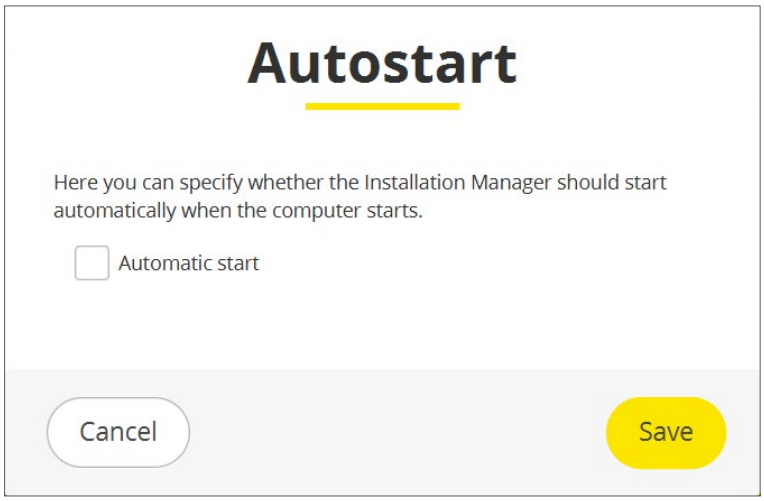
The settings made under “Settings and support” only apply to Xesar systems on a PC.



15.3.1 Autostart

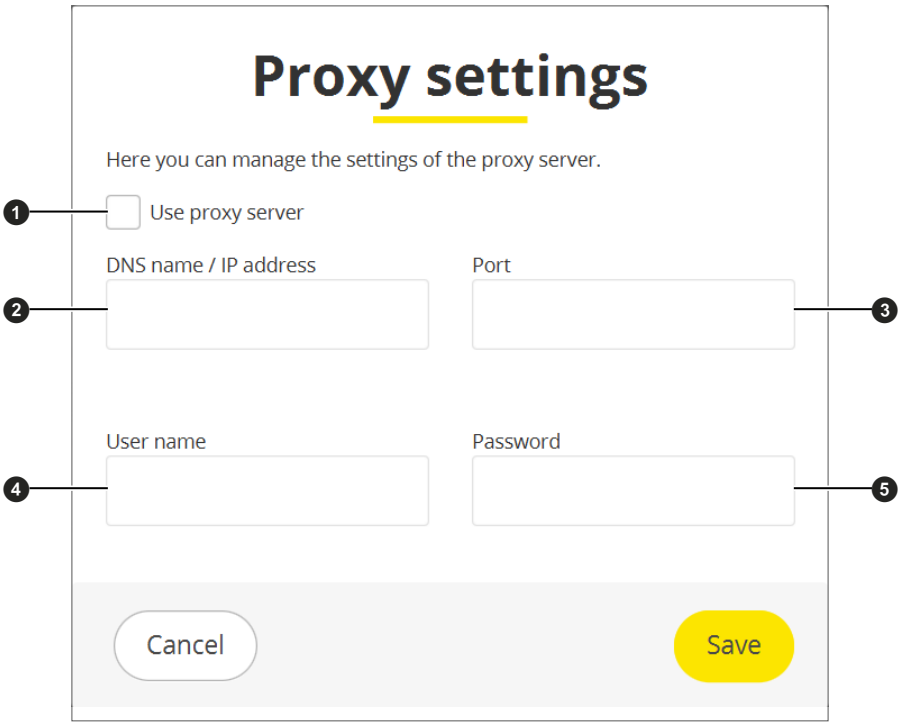
If the autostart function is activated, the installation manager and the running system are restarted automatically after a PC restart.

Activate Autostart if you are running online wall readers in your Xesar system on a PC.



15.3.2 Proxy settings

The corresponding settings can be made under Proxy Settings if required.



- Enable or Disable use of ❶ Proxy Server
- DNS name / IP address ❷ of the proxy server
- Port ❸: Proxy server port
- User name ❹: Proxy Server Username
- Password ❺: Proxy server user password

15.4 Restore/import

The following situations require a restore or import of a system:

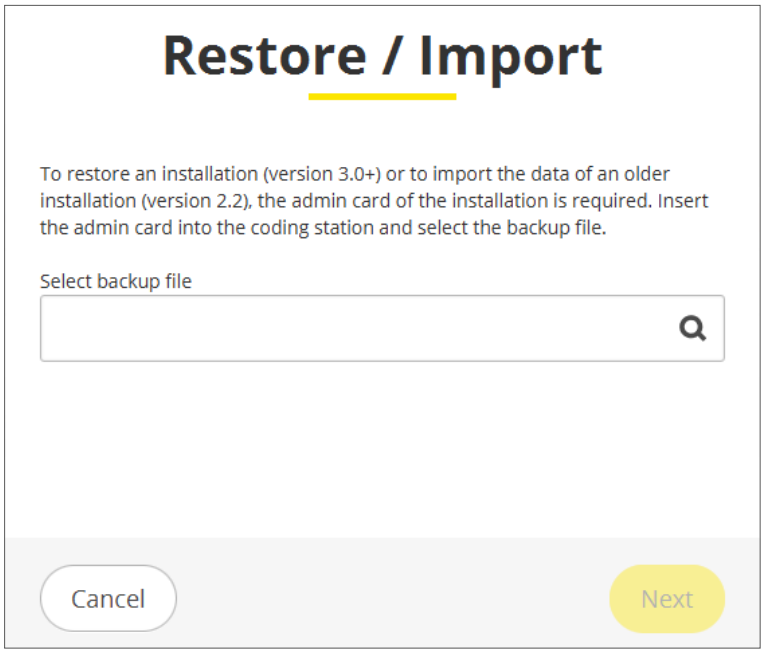
- Restore after a hardware or software failure.
- Transfer to a new hardware.
- Upgrade of an older system.

To upgrade or transfer the system, it is important that you **create a current backup file before restoring/importing**. Backup can be performed manually.

A system that is to be restored must NOT already exist in the Installation Manager.

To successfully restore/import a system, the following components are required:

- A backup file of the system that is as current as possible.
- The Admin Card belonging to the system to be imported must be inserted in the coding station.
- All systems in the Installation Manager must be stopped.

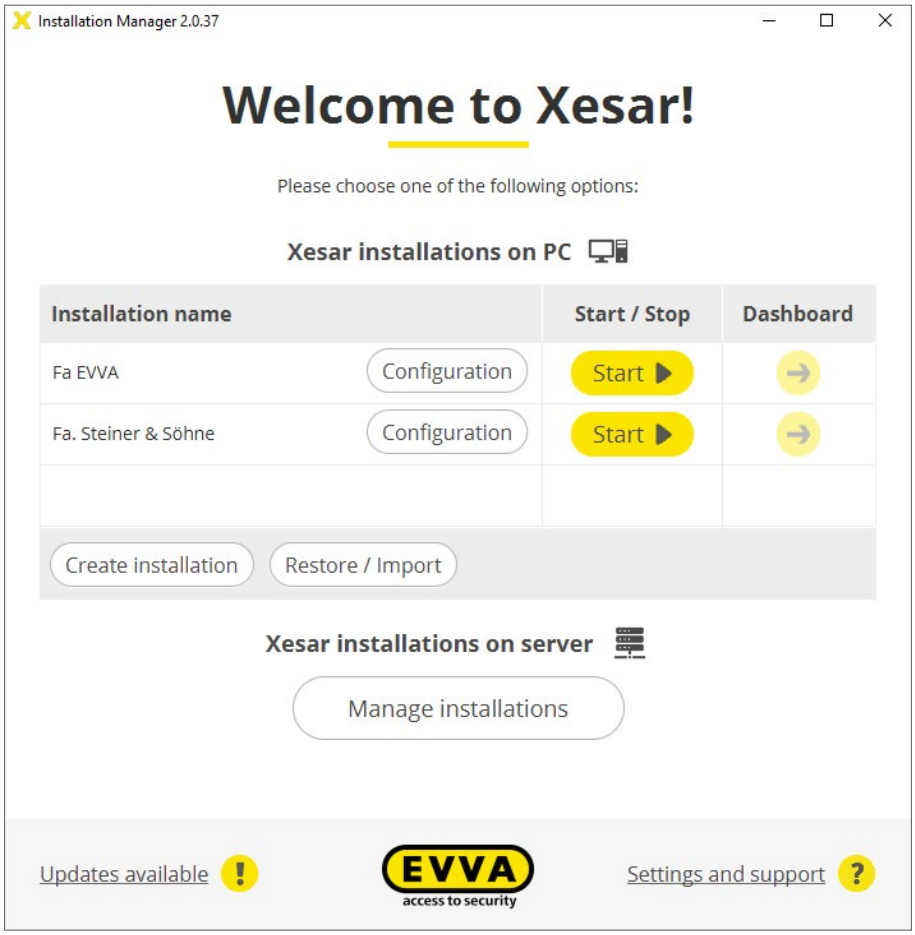


» Select the backup file to be restored or imported.
» Click **Import** and follow the instructions.

15.5 Update of installation manager and systems

The installation manager and the systems are updated separately.

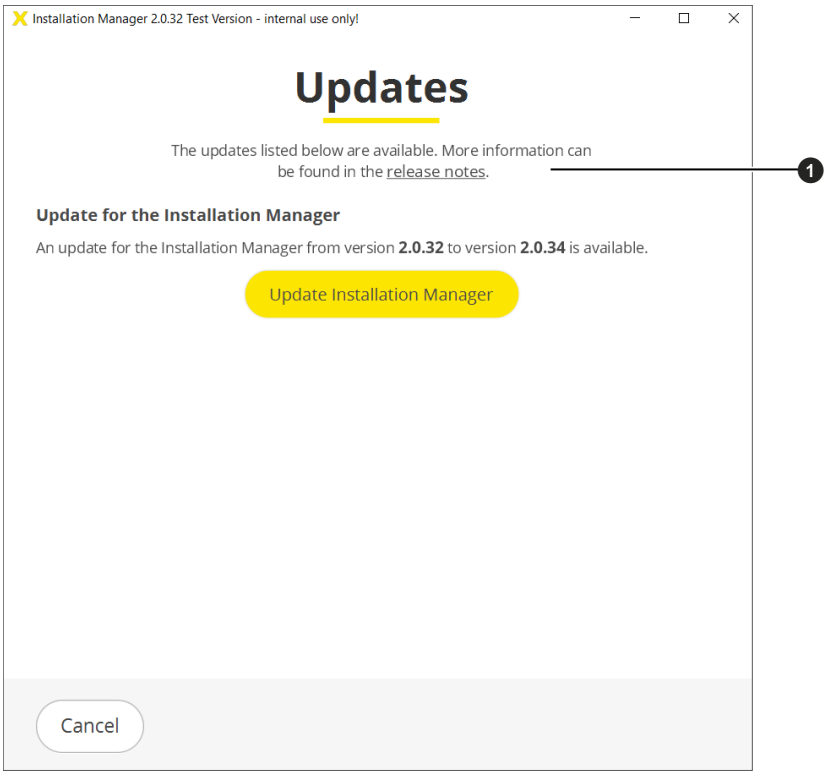
The installation manager and the system are updated in the installation manager.



Updates available : If updates are available, the note is highlighted.

» Click on **Updates available** to display the page with the available updates.

» Follow the instructions to perform the updates



The Updates page displays all available updates to the installation manager and the existing systems.

The "Release Notes" link ❶ takes you to the Release Notes with descriiptions of new features of the update versions.

» First carry out the update of the installation manager.
» Then carry out the update for the respective system.

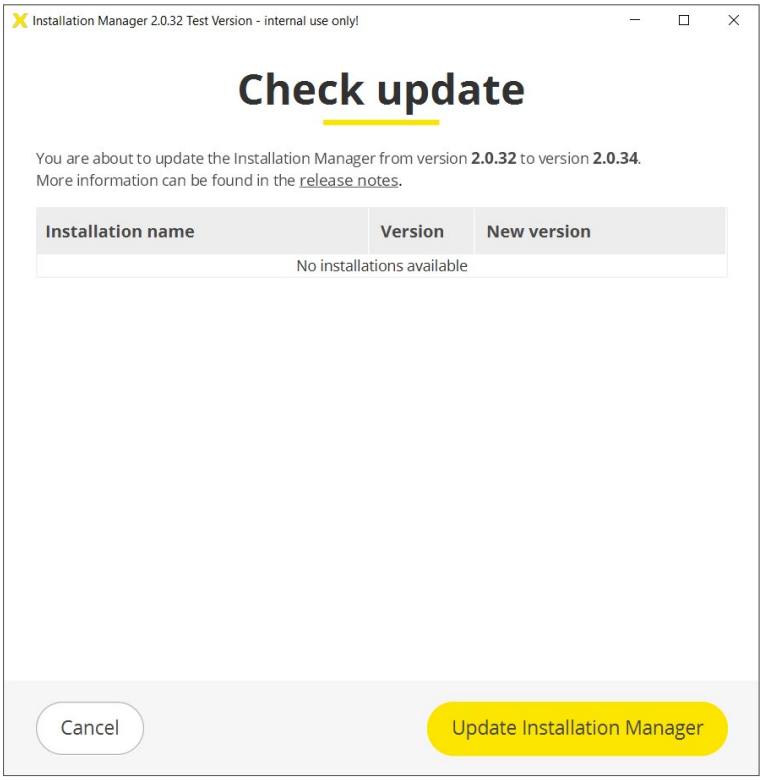
Check update: If no updates are displayed, click on the link to check whether new updates are available.

The date of the last update check ❷ is displayed.

In order to receive updates, the system PC must be connected to the EVVA server via the Internet.

15.5.1 Update Installation Manager

» On the "Updates" page, click the button **Update installation manager**.



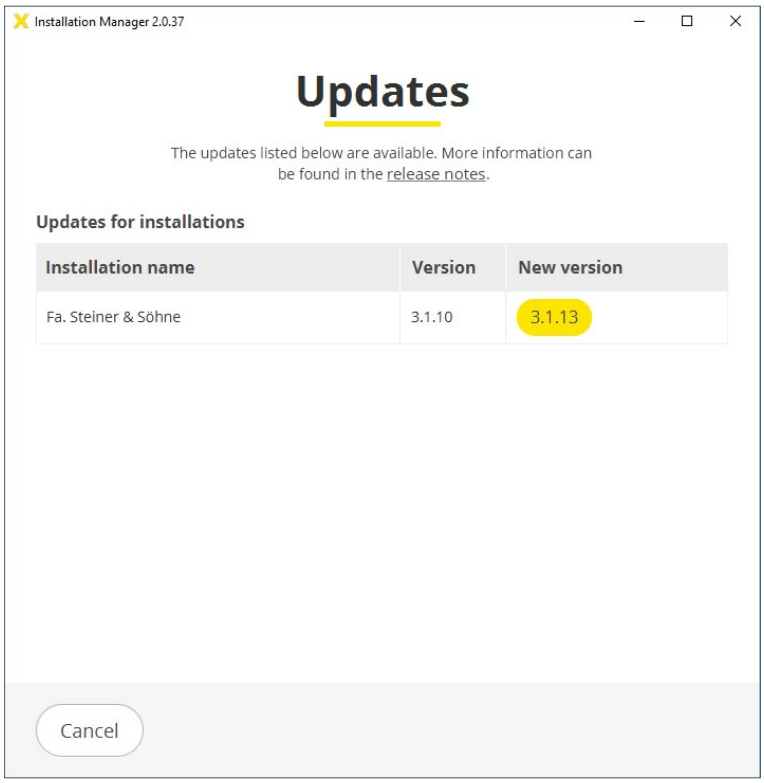
Before updating the installation manager, it is checked whether the existing version of the system can be updated with the new installation manager.

When the system is ready for the Installation Manager update, this is indicated in the "New version" column.

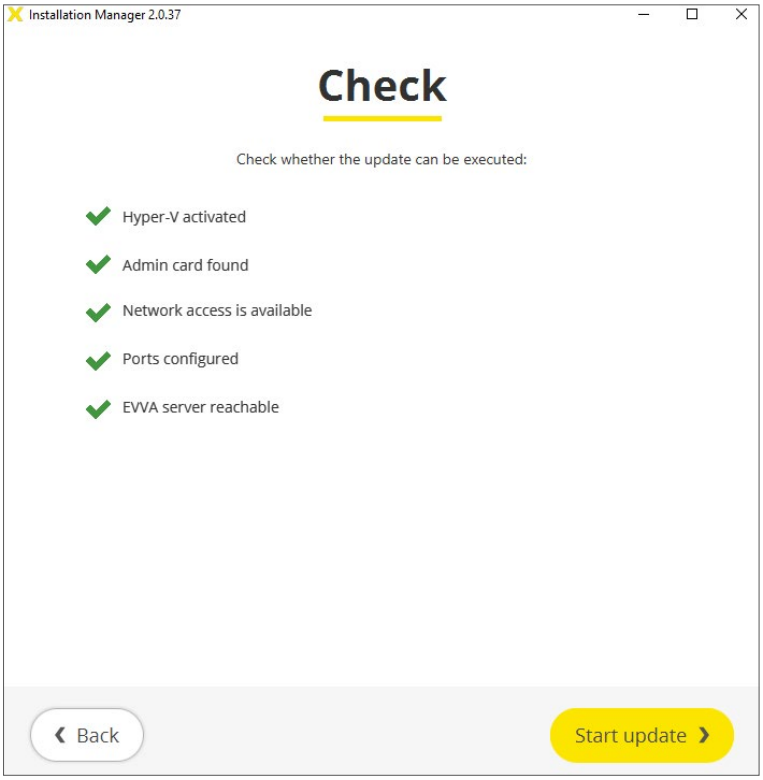
» Click the button **Update installation manager**.

15.5.2 Update of systems

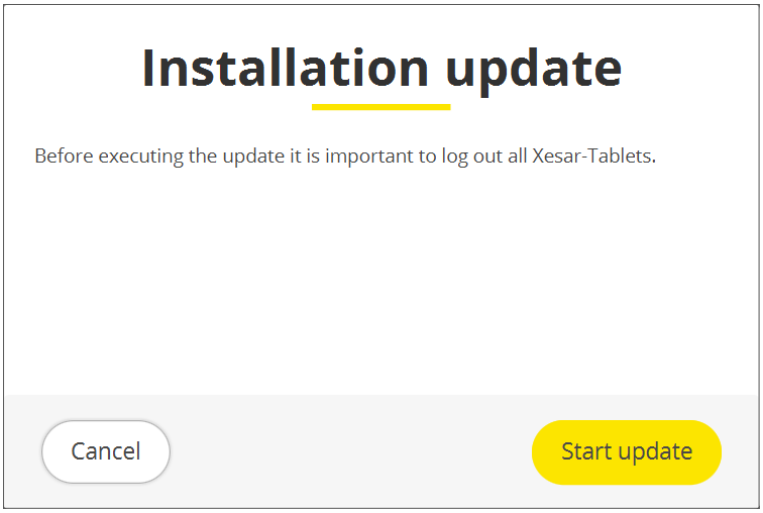
System updates are displayed on the system page in the column “New version”.



» Click on the respective version button.



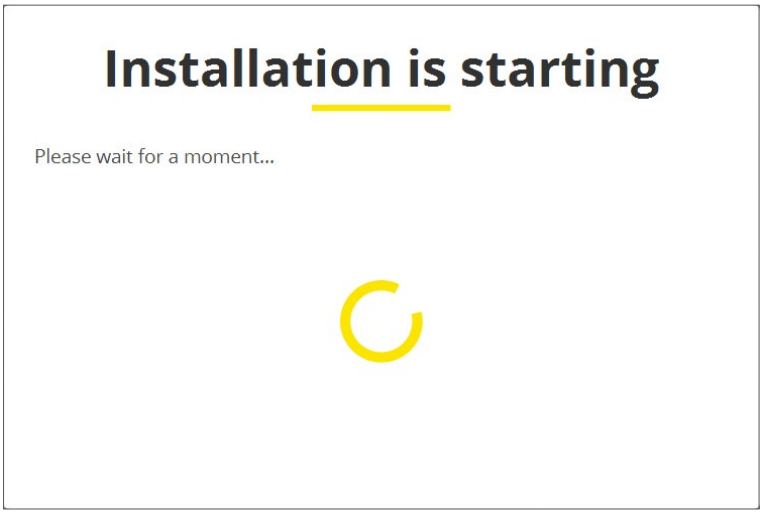
All necessary requirements and settings are checked before the update.



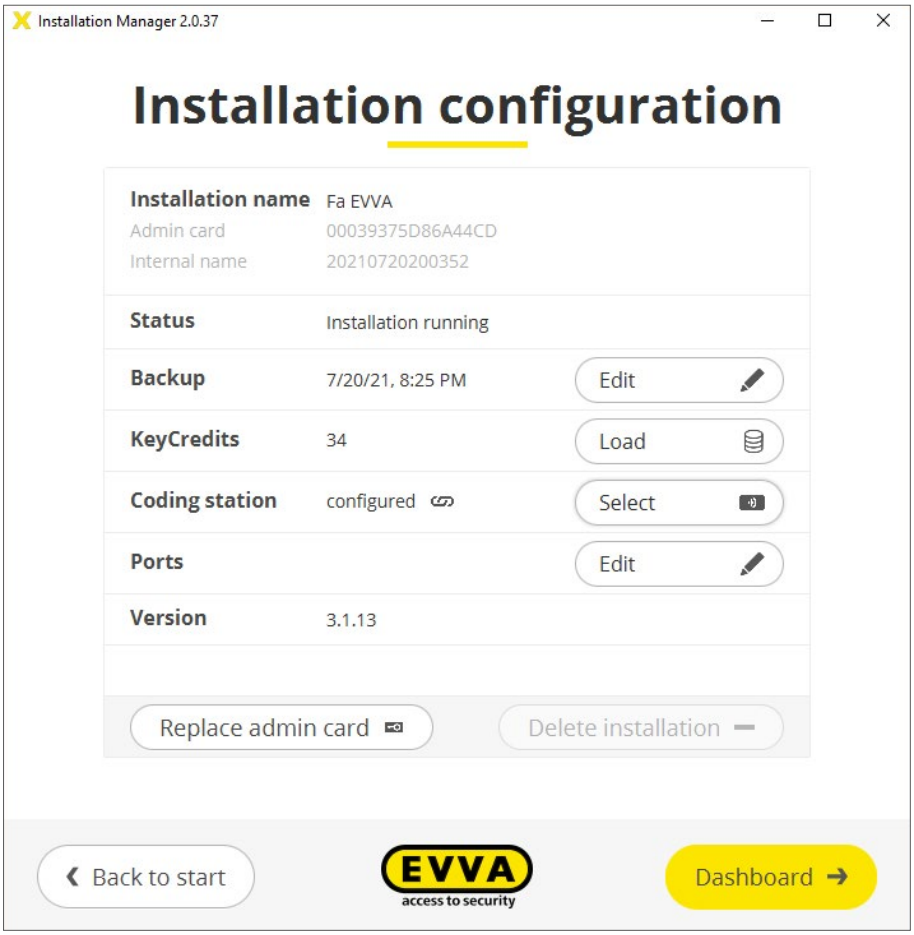
» When all requirements are met, click **Start update** and follow the instructions.

Before updating the system, each respective tablet must be logged out of the system.

A backup is made before the system is updated. To do this, the system must be started.



» Click **Start update** to update the system.

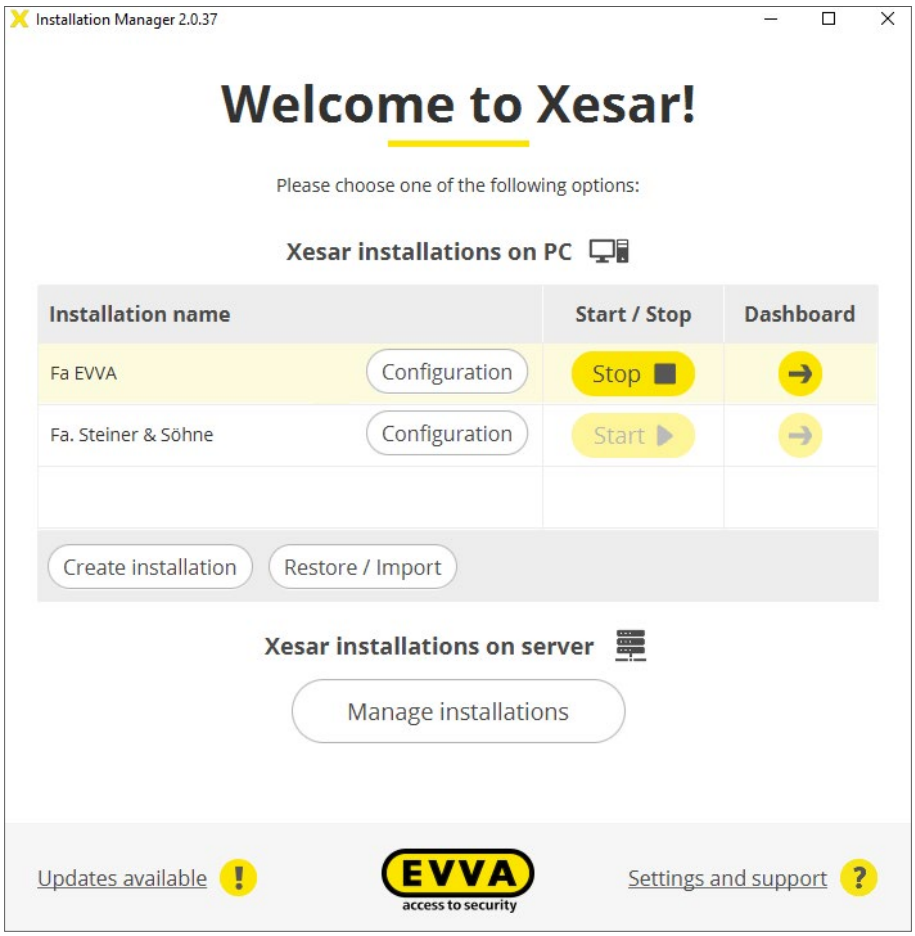


After a successful update, the current version number is displayed on the configuration page of the system.

15.6 Manage multiple systems on one PC

Several systems can be managed in the Installation Manager.

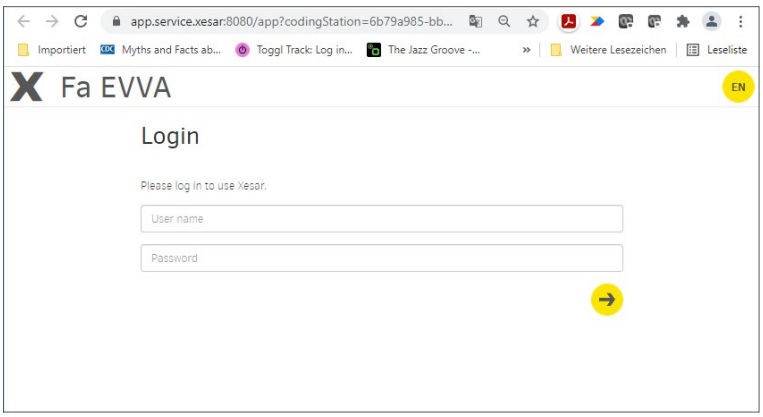
Only one system can be started.



» To create another system, click on the button **Create system** and follow the instructions.

15.7 Management of a started system

» Click on the button **Dashboard** to access the system login in the browser.



» Log in with the user name **admin** as the system administrator using the corresponding password from the system safety sheet.

After logging in as admin, you can change the password and create additional users in the “Users” tile.

System administrator (su) can only change user passwords.

16 Xesar systems on server

16.1 Installation requirements

Docker and the driver for the coding station must be installed on the system PC (Windows 10 Pro) before beginning the installation of Xesar 3.0.

16.2 Programs for installation and management

To create and manage Xesar systems on servers, you require the following programmes:

16.2.1 Installation manager

You can manage one or more systems with the Installation Manager. In addition, Xesar system settings can be configured.

The following tasks can be performed:

- Easy creation of Xesar systems on PC or server
- Starting and Stopping a system
- Admin Card management
- Performing updates
- Management of multiple systems.
- Add KeyCredits and KeyCredit Xesar Lifetime
- Setting up automatic backups of the started system
- Replacement of defective Admin Cards
- Setting of system ports

16.2.2 Periphery Manager

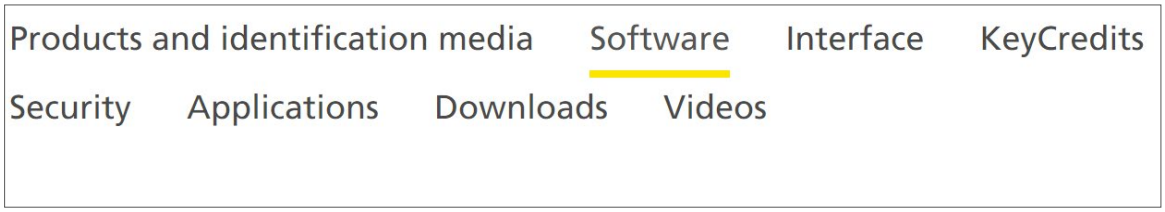
The Peripheral Manager permits the operation of a coding station on an administrator PC and on client PCs in a multi-user system.

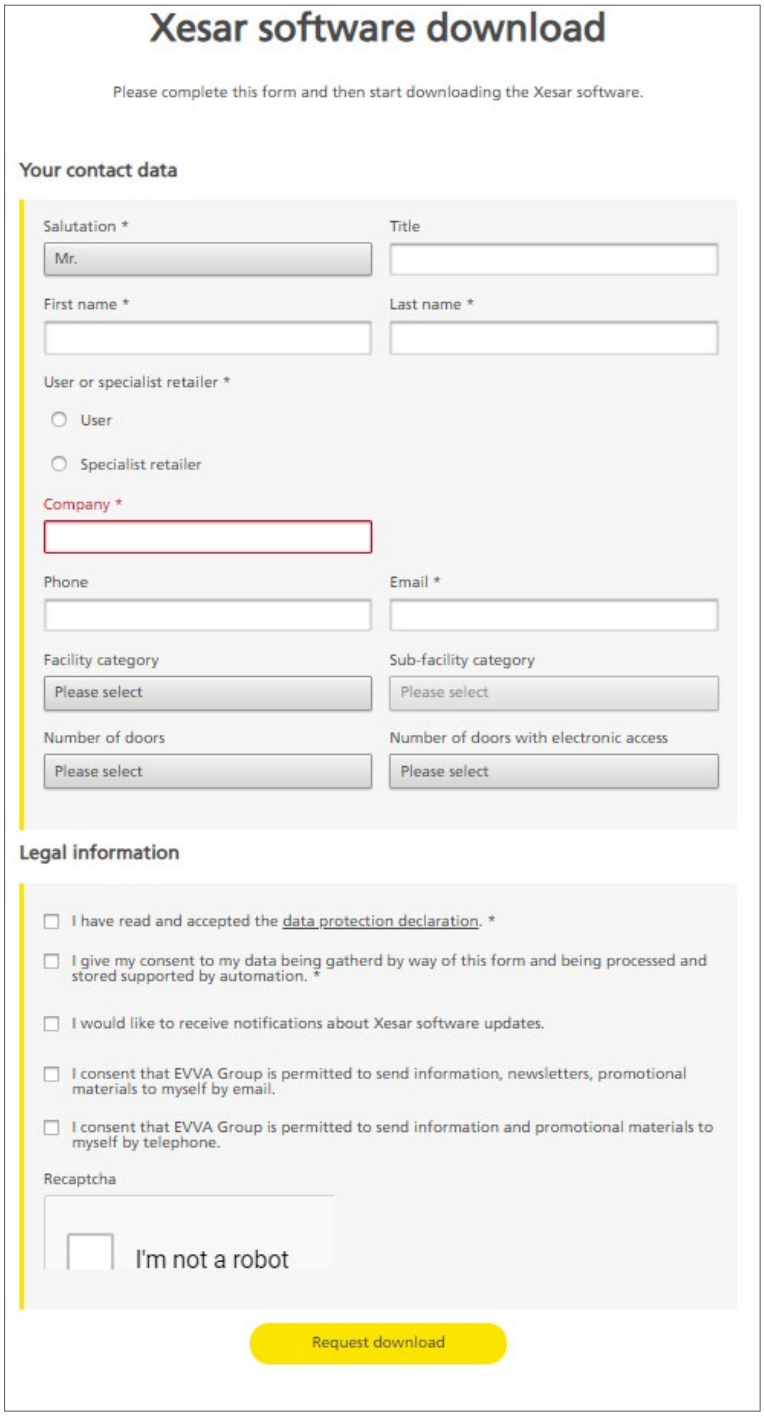
The Periphery Manager can be downloaded from the **Xesar software > Support > Updates**.

16.2.3 Xesar software

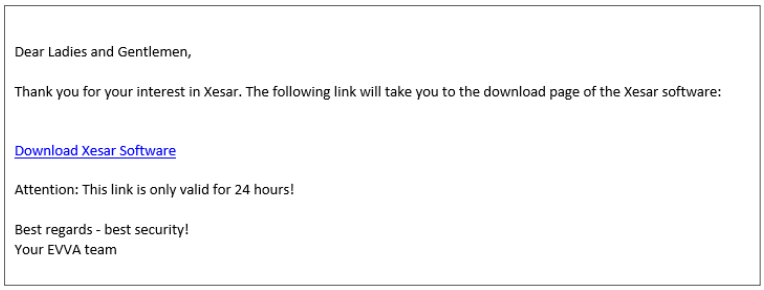
The Xesar software is an application that is started from the installation manager and runs in a browser. The Xesar software can be used to manage a system started in the Installation Manager on the dashboard.

You can download the current installation manager from the EVVA website by clicking on the Software tab.





» Complete and submit the "Download Xesar software" form.



Dear Ladies and Gentlemen,

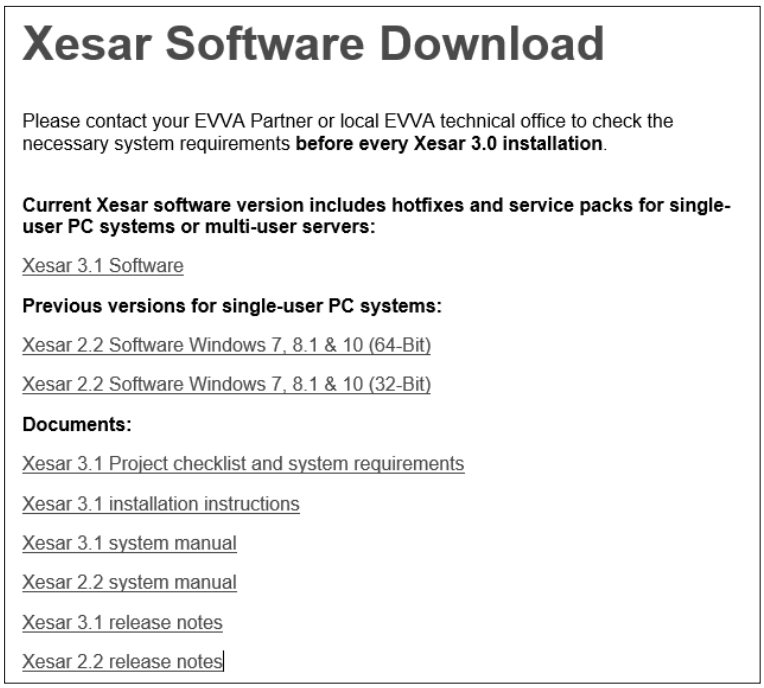
Thank you for your interest in Xesar. The following link will take you to the download page of the Xesar software:

Download Xesar Software

Attention: This link is only valid for 24 hours!

Best regards - best security!
Your EVVA team

You will receive an email with a temporary download link to the email address you provided in the "Download Xesar Software" form.



Xesar Software Download

Please contact your EVVA Partner or local EVVA technical office to check the necessary system requirements **before every Xesar 3.0 installation**.

Current Xesar software version includes hotfixes and service packs for single-user PC systems or multi-user servers:

Xesar 3.1 Software

Previous versions for single-user PC systems:

Xesar 2.2 Software Windows 7, 8.1 & 10 (64-Bit)

Xesar 2.2 Software Windows 7, 8.1 & 10 (32-Bit)

Documents:

Xesar 3.1 Project checklist and system requirements

Xesar 3.1 installation instructions

Xesar 3.1 system manual

Xesar 2.2 system manual

Xesar 3.1 release notes

Xesar 2.2 release notes

- Load the current Xesar software onto your PC.
- Double-click to open the *.msi file.

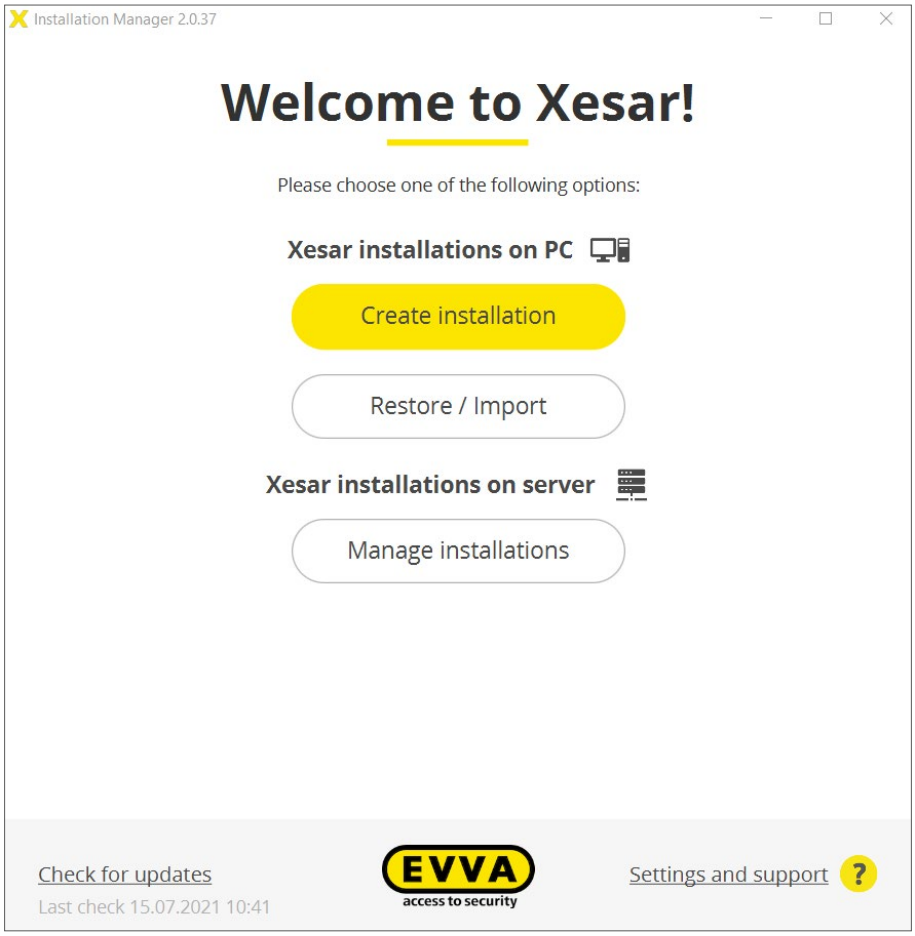
The Installation Manager is installed and a desktop and start menu shortcut is created.

- Start the Installation Manager by clicking on one of the links.

16.3 Installation procedure

» Start the installation manager EXE file.

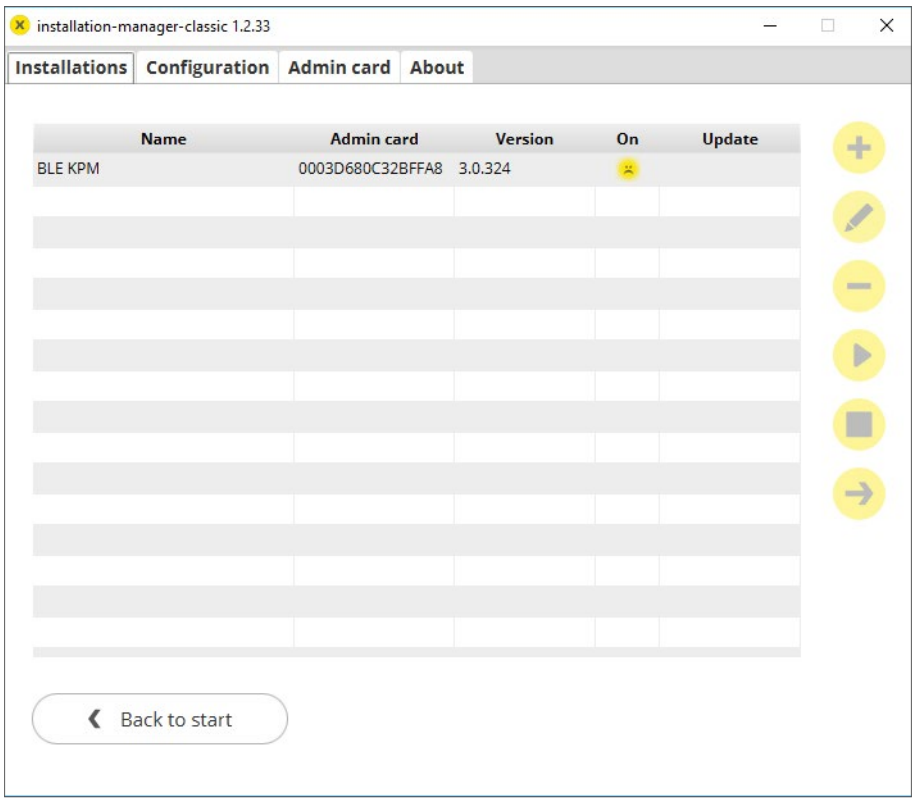
"Welcome to Xesar!" window offering installation selection of Xesar systems on PC or server:



16.3.1 Installation of Xesar system on server

» Click the button **Manage server system**, to access the Management view of systems on the server.

When updating to the new Installation Manager, existing Xesar systems on servers are automatically imported into the Xesar system management view on the server.



Xesar systems are managed on servers in accordance with the following instructions.

16.4 Starting and quitting Xesar systems on server

» Click on the link provided by your administrator (server)

or

» Click on the **Goto** symbol in the Xesar Installation Manager or Xesar Periphery Manager.

Close the Xesar Periphery Manager before you shut down the client PC (important for the coding station).

» Click on the **Stop** symbol, to disconnect the Xesar Periphery Manager from the browser.

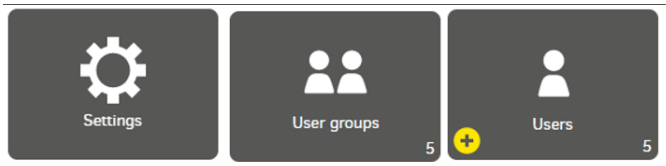
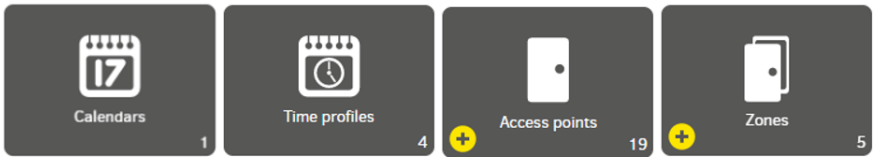
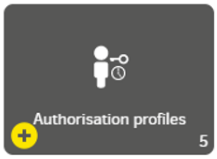
» Right-click the symbol **Exit** , to close the Xesar Periphery Manager.

The Xesar Periphery Manager symbol is in the taskbar.

The Xesar Periphery Manager is not closed when you click the **x** symbol in the program window.

If you do not exit the Xesar Periphery Manager correctly, an error may occur the next time you start the Xesar Periphery Manager. In such a case, the Xesar Periphery Manager must be reconfigured.

17 Commissioning Xesar software

1st Step	
2nd Step	
3rd Step	
4th Step	

17.1 General information on commissioning

New settings and changes must be saved before leaving the respective screen. If this is not done then the original settings are retained.

Click on the **csv** or **xlsx** icon. All lists can be exported and printed as .csv or .xlsx files. The original file must use 65001: Unicode (UTF- 8) is used.

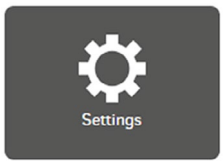
Mandatory fields are marked *****.

Clicking on the **?** icon displays the corresponding help text.

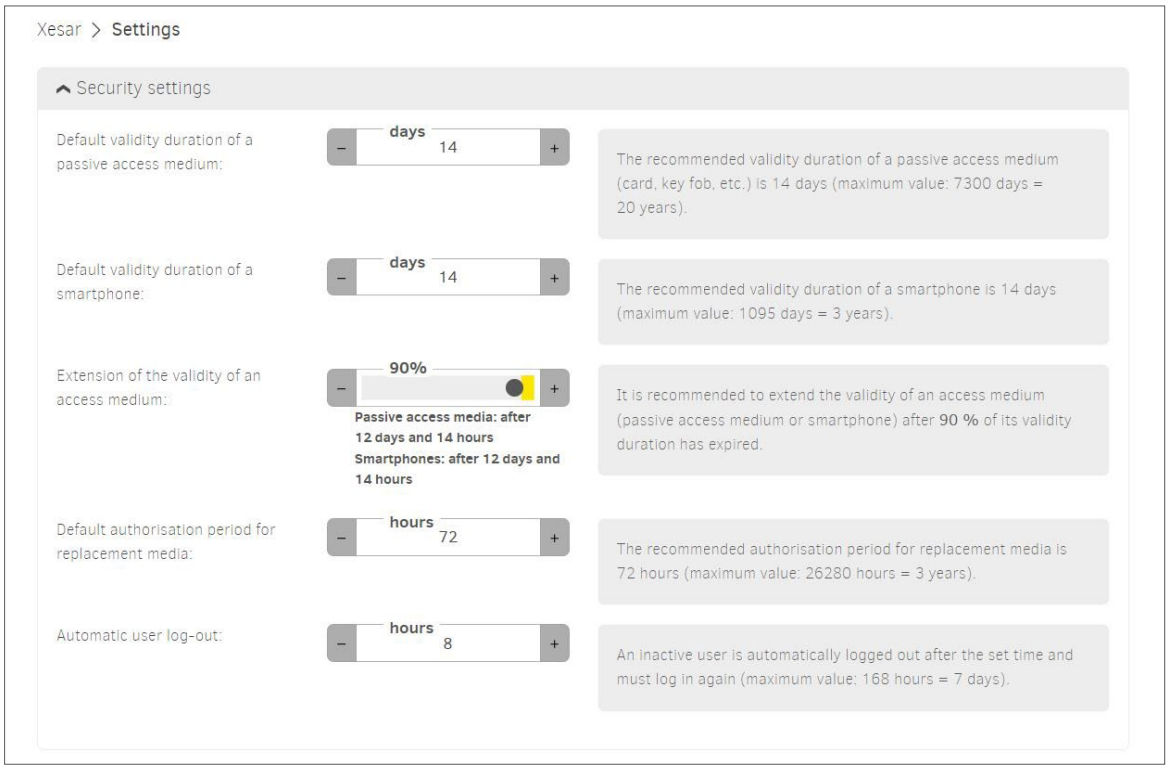
Double-clicking on the column divider adjusts the column width to the column header.

The resulting formatted list depends on the number of columns and the screen display.

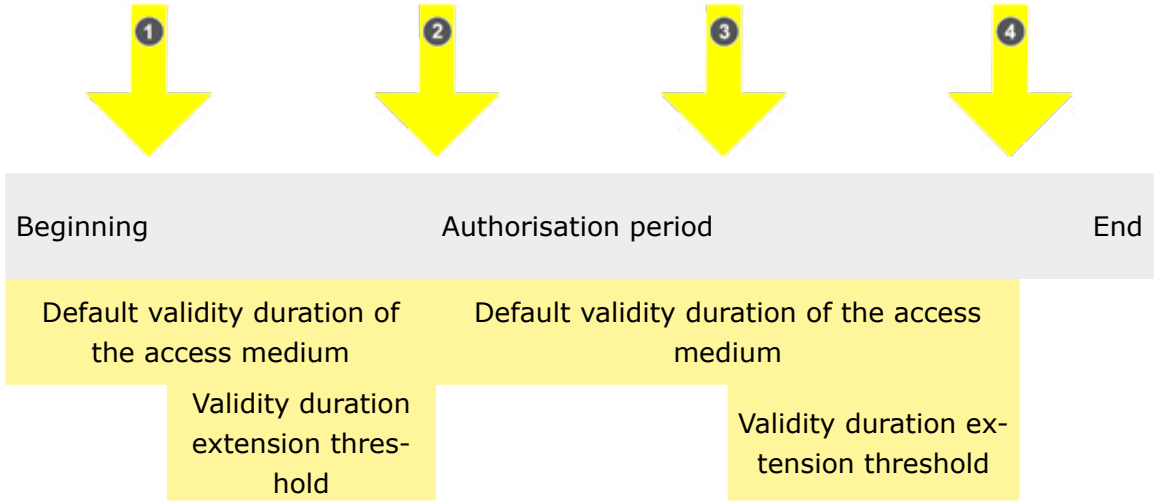
17.2 Settings



17.2.1 Security settings



17.2.2 Validity duration and authorisation period of the access media



❶ Earliest possible Update
❷ Latest possible Update
❸ Earliest possible Update
❹ Latest possible Update

Standard validity duration of the access medium

The standard validity duration is the preset period during which the access medium is valid after it is updated on the coding station or Xesar online wall reader.

The standard validity period can be set individually when issuing access media. Once the standard validity period has expired, the access medium becomes invalid and may need to be updated at the coding station or on the Xesar online wall reader. The shorter the standard validity period, the more secure the system is, as the access medium becomes invalid sooner.

Standard validity period of a smartphone:

The standard validity period is the preset period during which the smartphone is valid as an access medium after updating via the Xesar Mobile Service (XMS).

The standard validity period can be customised in the Xesar software.

When the standard validity period has expired, the access medium becomes invalid and must be updated via XMS. This is done automatically as soon as a connection to the Xesar system is established.

The shorter the standard validity period, the more secure the installation is, as the access medium becomes invalid sooner.

The recommended validity duration is 14 days.

The maximum validity duration that can be set is 7300 days (approx. 20 years) for passive access media and 1095 days (approx. 3 years) for smartphone.

Extension threshold for the validity duration of an access medium:

The extension threshold of the validity duration defines the time range in which the validity duration of the access medium is extended at the coding station or the Xesar online wall reader.

It is recommended to extend the validity of an access medium (passive access medium or smartphone) after 90 % of its validity duration has expired.

Default authorisation period for replacement media:

According to the system default setting, the standard authorisation period for replacement media is 72 hours. The default authorisation period can be set individually when issuing replacement media (see chapter “Access media”).

Automatic user logoff:

For security reasons, the user (e. g. receptionist, administrator or maintenance technician) is automatically logged out of the user login (user and login) after the preset period of time. To be able to operate the Xesar software, the respective user must log in again.

17.2.3 System settings

IP address of the server:

The IP address is required to connect the coding station to the server (the IP address is written to the configuration file). The IP address is also required when adding a coding station to the system.

In the case of local installation, the IP address of the local installation is automatically displayed in the input field.

Daily execution time:

The daily execution time is the time of system time synchronisation. In addition, the daily execution time is used for the following Xesar online wall reader configuration settings with the Xesar software (backend).

- Complete blacklist transfer to the online wall reader. Securely blocked access media are removed from the blacklist.
- Personal event entries are anonymised after the defined time has elapsed.
- Maintenance tasks are generated three months before the first time changeover in the year.
- Creation of maintenance tasks to update the calendar days on the components.
- The backup status is updated.

Always select a time as the daily execution time when the system is running and the Xesar online wall reader is online (e.g. office hours)!

Logo:

The logo is displayed on the dashboard in front of the names of the installations. If you want to add a custom logo, please note the following specifications:

Maximum file size: 2 MB
Possible file types: jpg, png, gif, svg

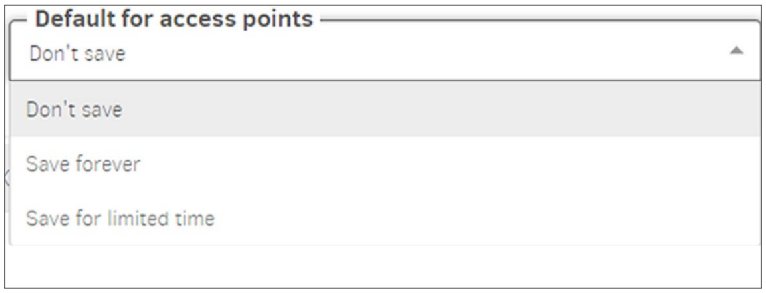
Settings relating to personal data:

The personal reference settings specify if and how long personal event data is stored.

> When entering the settings, note your company's data protection requirements.

There are three data storage settings for persons and access points:

- Don’t save
- Save forever
- Save for limited time (setting range in days)



Person and component-specific settings are defined in the tiles “Persons” or “Access points – Component”.

Settings for the Xesar tablet:
For security reasons, the use of the Xesar tablet for system-related maintenance tasks is protected by a PIN code. The PIN code request on the tablet can be deactivated.

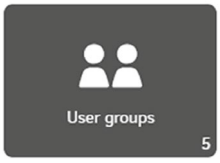
Management of data on the Xesar Tablet:
Data should be retained even after the tablet is switched off.
This is useful if it is not possible to establish a WLAN connection between the tablet and the system at the installation where the components are installed.

Important:
When the function is activated, safety-relevant data are available on the tablet. Make sure that the tablet is only operated by authorised persons.

Change the preset PIN code when you use the Xesar tablet for the first time.

17.3 User groups:

The authorisations for users are defined within the user groups.



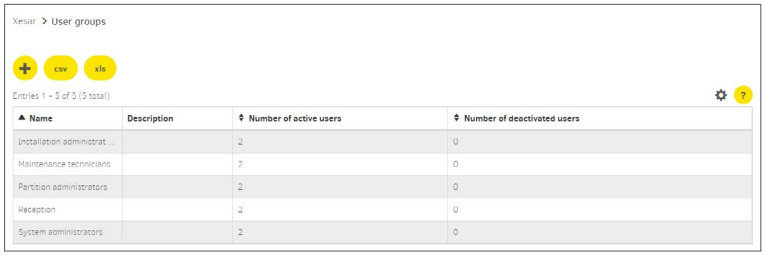
Users manage the system using the Xesar software. Any number of users can be created with various authorisations (depending on their function). These different authorisations are defined in the user groups.

Depiction of all predefined user groups:

Users can be assigned to predefined user groups. User groups that have been predefined cannot be deleted.

A user can be assigned to multiple user groups.

Note: If a user is assigned to several user groups, the authorisations for the corresponding user are cumulative.



The following predefined user groups are available for selection:

System administrator
may modify user passwords

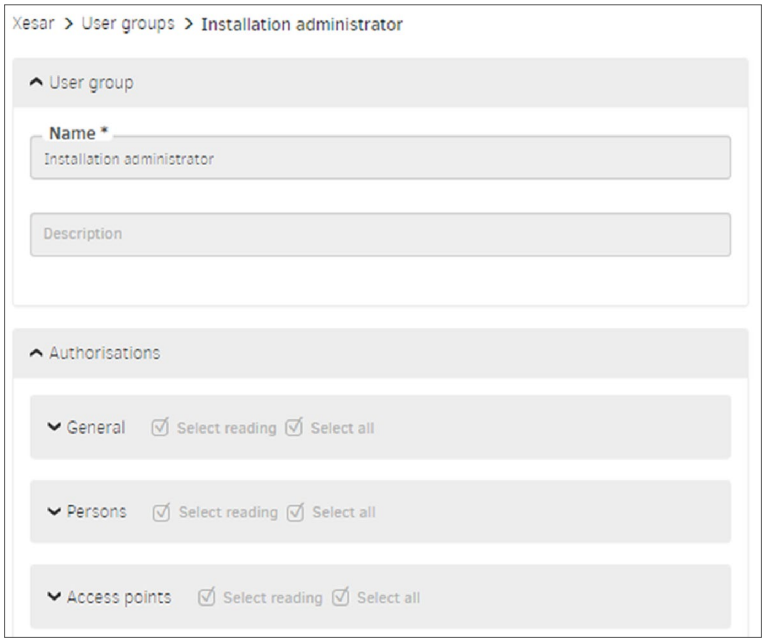
Installation manager
has all authorisations but may not change user passwords

Maintenance technician
has limited, maintenance-relevant authorisations

Partition manager
has limited, administration-relevant authorisations

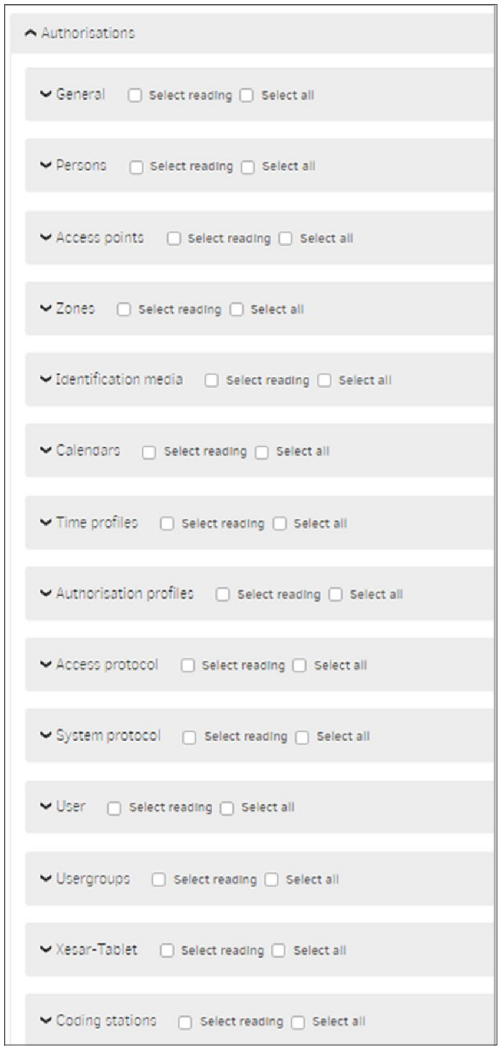
Front desk
has limited, reception-relevant authorisations

Example: installation manager user group
The users in the user group have all read and edit permissions:



The authorisations of these predefined user groups cannot be changed.

If required, copy a predefined user group and change the authorisations.
Give this individual user group a meaningful name and save it.

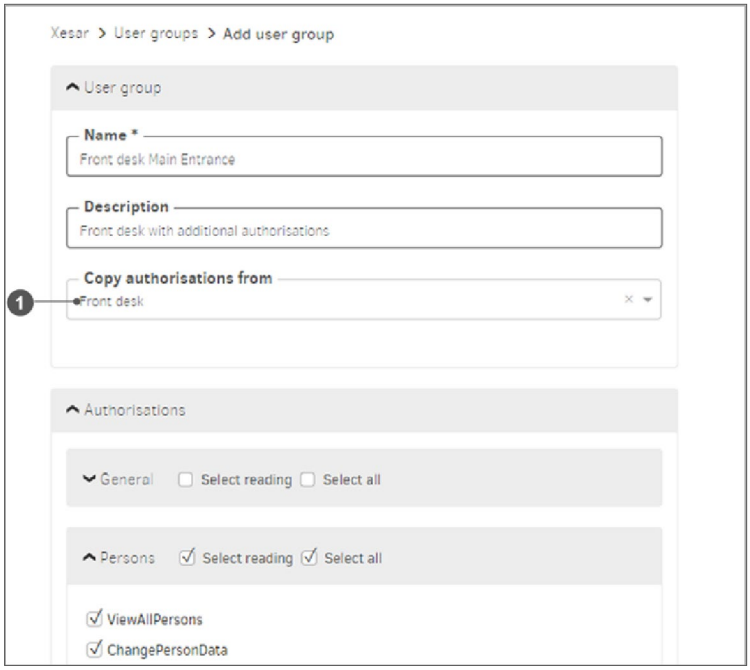


The authorisations are grouped as tiles on the dashboard.

The following authorisations are defined in each authorisation group:

- read-only authorisations
- all authorisations are selected.

For example, the individual user group "Front desk main entrance", has rights of the basic front desk user group ❶ and additional reading and editing rights for persons settings:



Use the predefined user groups as the basis for assigning authorisations to users.

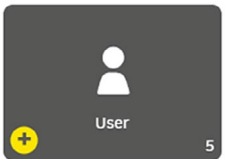
Special authorisation groups can be generated as required. In such cases, please contact the EVVA Technical Office.

Possibility to restrict admission authorisation profile:

Only designated authorisation profiles can be assigned by users belonging to the respective user groups.

Example:
For example, users in the user group front desk may only assign access media to the authorisation profiles of employee, trainee, cleaner and shift worker. Users in other user groups may also assign the authorisation profiles supervisor, assistant, fire brigade and master key to an access medium.

17.4 Users



Users manage the system using the Xesar software. Any number of users can be created with various authorisations (depending on their function).

A new user can be added using the '**Add**' icon. The number of registered users is displayed in the User tile.

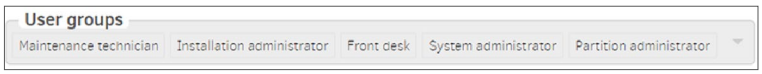
Users are also persons who have access authorisations in the system with access media assigned to them.

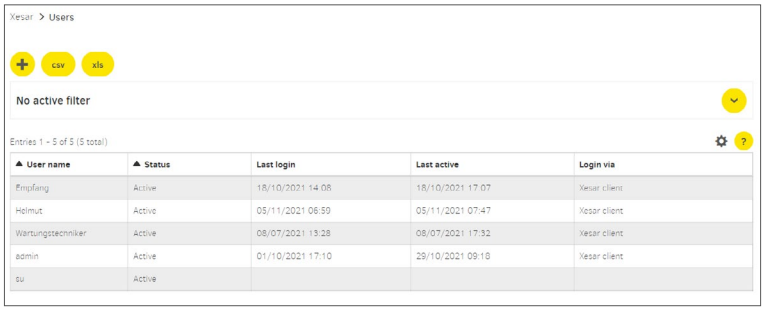
All registered users are displayed in the user overview list.

The users **su** (super administrator) and **admin** (administrator) that were created during the initial installation cannot be changed or deleted.

- **su**
  the system administrator is the only person authorised to change passwords

- **admin**
  has all rights





New users:

If you want to create a new user, the following input fields are available for this purpose:

Mandatory fields are marked with *.

User name
for the new user, e.g. Administrator 1

Description
additional information about the new user

Password
for login.
At least 6 characters; additionally, an evaluation of the security level of the password is shown.

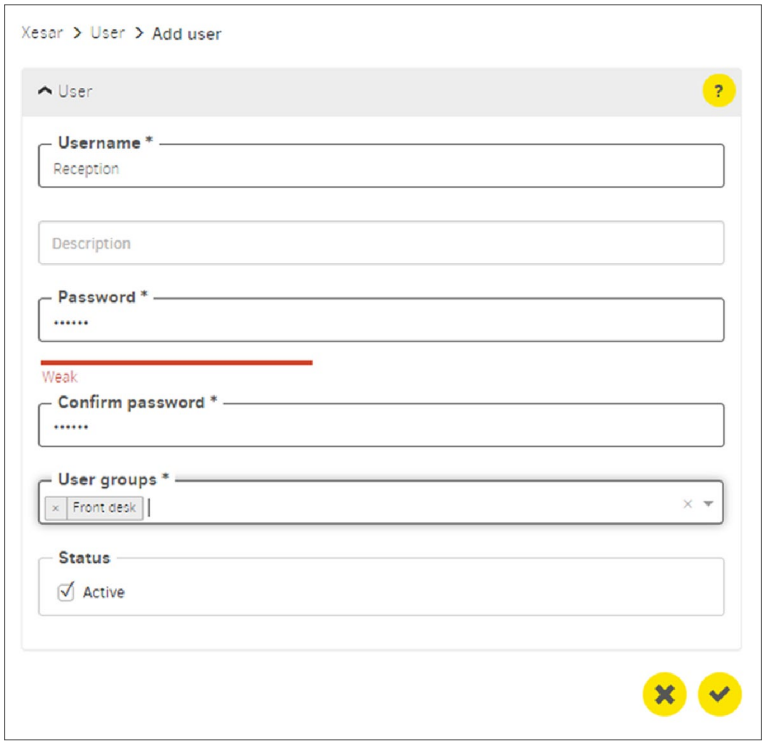
Re-enter password
Re-enter the selected password.

User groups
Selection of the user groups defined for the user. At least one user group must be selected.

Person
(This field is only displayed after saving for the first time)

The user function can be assigned to an individual, e.g. maintenance technician1 > Hans Huber.
The personal reference has purely informational value and no functional effects.

Status
Users can be set by admin to active or inactive. Inactive users cannot log in.



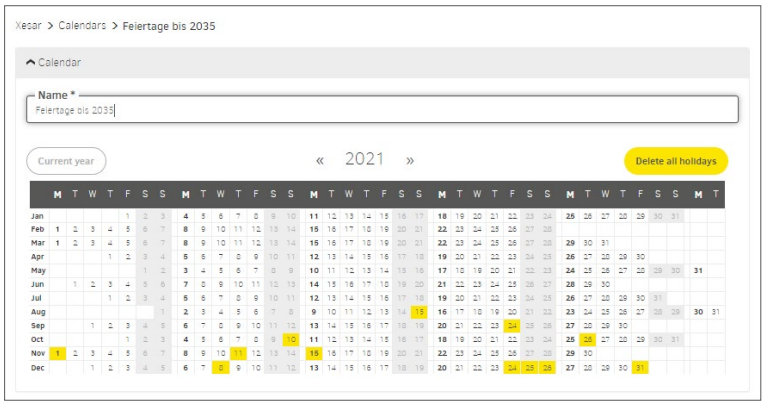
Download configuration
The respective user certificate (configuration) is downloaded. The user certificate is required for secure third-party system interface actions (e.g. personal data import via the third-party system interface).

17.5 Calendar

Use the calendar function to manage holidays, such as public holidays or company holidays within a calendar year. Exceptions to time profiles are possible on these holidays. The number of calendars is displayed in the Calendar tile.

A maximum of 5 calendars with a total of 50 different holidays can be defined.

A holiday (e.g. Christmas) may only occur in one calendar.



Import calendar

You can import and further process existing calendars in the file format .ics or .csv.

You cannot import calendars where the current day is marked as a holiday.

17.6 Time profiles:

Both office mode time profiles (automatic permanent opening for Xesar access components) and time profiles for authorisation profiles of persons or access media, are defined in time profiles.

Additionally, times for the automatic closing of a manual office mode (manual permanent opening) are defined.

If no office mode time profile is assigned to a Xesar access component, only authorised access media have access.

If no time profile is used when creating an access medium, no access time restriction applies to this access medium – the access medium therefore has permanent access.

Office mode:

The Xesar office mode allows access components to have automatic and permanent time-controlled access. In office mode, Xesar components allow access in the defined time slot even without an access medium.

Example:
A business premises is open from 8:00 am to 4:00 pm. The office mode time profile is from 8:00 am to 4:00 pm.

Access through the entrance door of the business premises with this time profile is available to all persons without an access medium between 8:00 am and 4:00 pm. The Xesar access component automatically switches to **Open** at 8:00 am and to **Close** at 4:00 pm.

Office mode can be terminated manually at any time with an authorised access medium.

Shop mode:

Shop mode is an extension of office mode. Office mode is not started automatically at the defined time, but only after a one-time identification with an authorised access medium.

Example:
An office mode with a time slot of 8:00 am to 4:00 pm has been defined for a shop. Additionally, shop mode is activated on the Xesar access component of the entrance door.
If an employee with an authorised access medium is late and is not in the shop before or at 8:00 am, the entrance door remains closed despite office mode. Only when the employee arrives at the shop (even after 8:00 am) and opens it with an authorised access medium, will office mode be started.

This prevents office mode from automatically opening the door even when no employee is present.

Manual office mode:

Within Xesar, manual office mode means the manual activation of a permanent release of Xesar access components. For the function, both the corresponding Xesar access component and the corresponding access medium must be authorised via the authorisation profile. Set the manual office mode in the respective menu item under **Access point** and **Authorisation profile**.

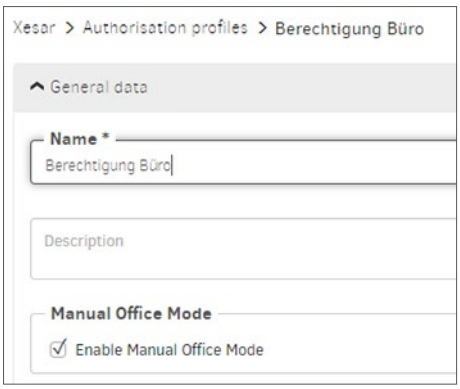
Manual office mode is activated by holding an authorised access medium to the Xesar access component twice. A corresponding visual and acoustic confirmation is issued (see system manual, chapter 'Event signalling').

Manual office mode is ended automatically at the defined closing time or manually by holding an authorised access medium at the Xesar access component twice. A corresponding visual and acoustic confirmation is issued (see system manual, chapter 'Event signalling').

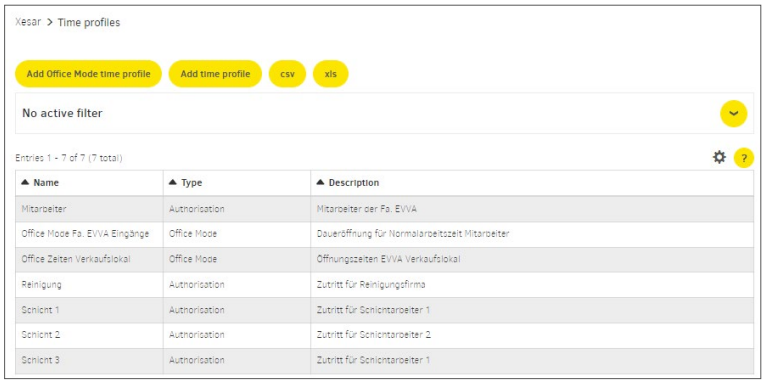
Activating manual office mode and shop mode:

» Open **Xesar > Access points > Main entrance**

» Open X**esar > Authorisation profiles > Users**



Time profiles view:



The times in the input fields can be entered numerically or using the arrow keys.

17.6.1 Add office mode time profile

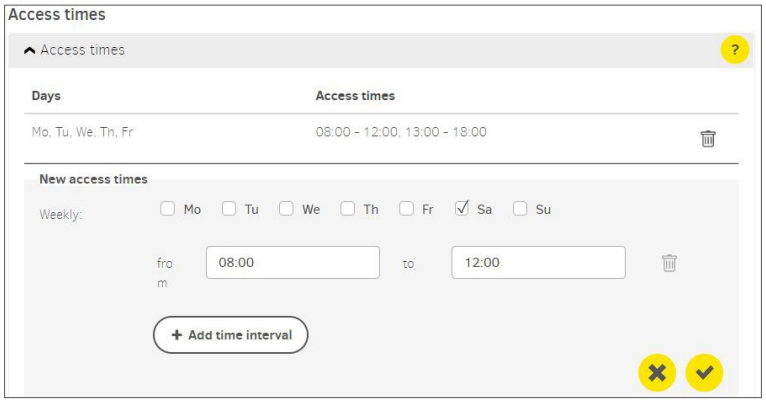
The “permanent opening” function is available for Xesar access components.

Access without authorisation is possible at defined times. The Xesar access component is then ready to open the door.

You can create a maximum of 24 time slot series.

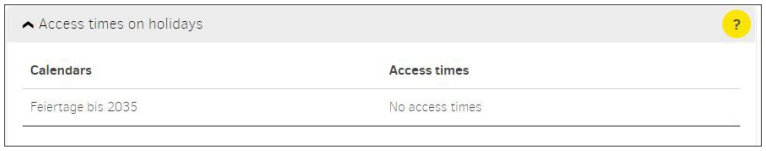
In total, a maximum of 5 different time slots or times per weekday or calendar can be added.

Example – office hours:
Monday to Friday from 8:00 am to 12:00 noon and 1:00 pm to 6:00 pm and Saturday from 8:00 am to 12:00 noon.



Holiday access times define deviations from time slot series within which modified access times or access prohibitions apply.

"No access times" means that no access is possible on holidays defined in the calendar. All existing calendars are displayed.



Automatic closing times:

Automatic closing times define times at which the manual office mode (manual permanent release) ends automatically. This ensures that a manually started office mode is safely terminated at the defined time.

The manual office mode can only be activated at defined Xesar access components and with authorised access media by holding the access media to the Xesar access component twice.

A maximum of 35 time series are possible.

Example:
Closing time Monday to Friday, 8:00 pm each day

Automatic closing times on public holidays:

The closing time can be changed for holidays.

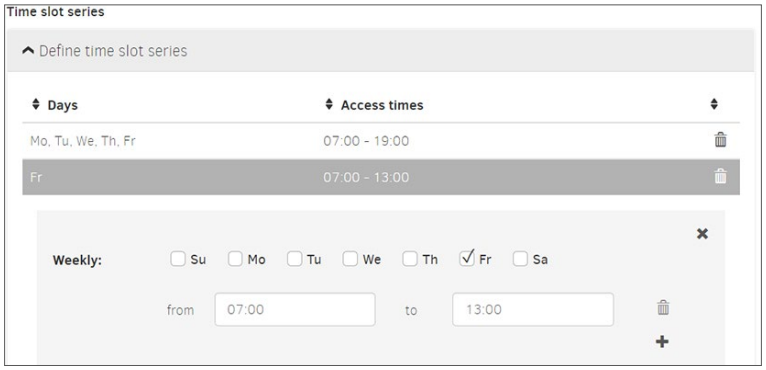
17.6.2 Adding a time profile

Time profiles can be added for persons and access media.

You can create a maximum of 24 time slot series.

Limits to authorisations:

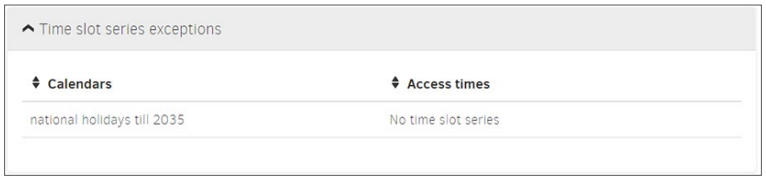
Example, access times for employees:
Monday to Friday from 7:00 am to 7:00 pm and Saturday from 7:00 am to 1:00 pm.



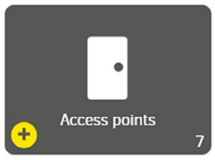
Time series exceptions:

Time slot series exceptions define deviations from time slot series, such as holidays, on which changed access times or access denials apply.

No time slot series means that there is no access on holidays defined in the calendar. All existing calendars are displayed.



17.7 Installation points



All access points with system access components are created and defined in the access points area. An access point can be a door or another application, e. g. lift.

List of access points:

Online status:
describes whether a component is online-capable and whether it is connected to the Xesar software

ID:
Unique identification (designation), e. g. room number according to building plan

Name:
Unique name or description, e. g. main entrance

Description:
user-defined description of the access point for a better understanding, e. g. central access, escape route to assembly point

Type:
user defined, e. g. glass door, locker or automatic door

Component type:
installed component at the access point

Bluetooth functionality:
describes the Bluetooth status of the component, e. g. without Bluetooth, Bluetooth activated, Bluetooth deactivated

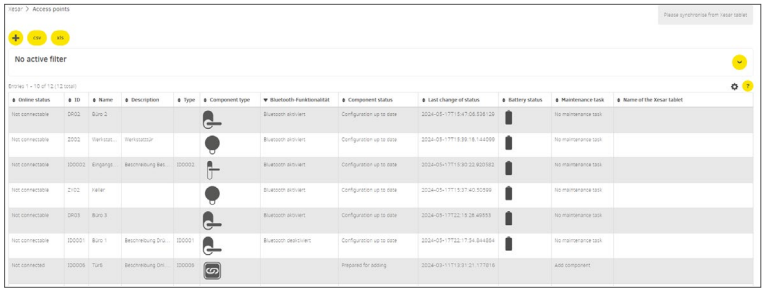
Life cycle status:
describes the current status of the component, e. g. prepared for adding

Last status change:
time of the last synchronisation of the component with the Xesar software

Battery status:
shows the battery status of the component: full or empty

Maintenance task:
Shows open maintenance tasks for the access point, e.g. component configuration, removal, add, firmware update

Name of the Xesar tablet:
Name of the tablet with the synchronised open maintenance task for the installation location



17.7.1 Add access point

Select the desired access component.

17.7.2 Describe access point

If you want to create a new access point, you can select from the following input fields:

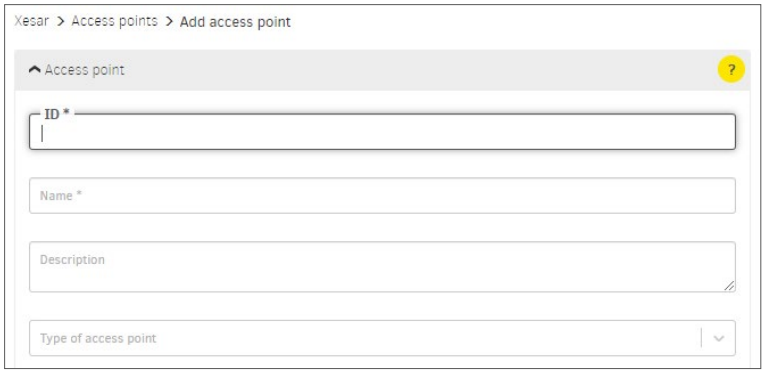
Mandatory fields are marked with *.

ID:
unique identification (designation), e. g. room number according to building plan

Name:
unique name or description, e. g. main entrance

Description:
user-definded description of the access point for a better understanding, e. g. central access, escape route to Wienerbergstraße assembly point

Type of access point:
user defined, e.g. glass door, locker or automatic door



Opening duration:
The opening duration defines the period of time that the access component will grant access after authorisation before disabling (locking) access again. The corresponding opening duration is **Short** or **Long**. The opening duration is defined for the respective person or access medium and triggered when authorisation is granted at the access component.

The assignment of the opening duration to the person or the access medium is carried out in the person and access media settings.

Time profile:
selection of the office time profile mode

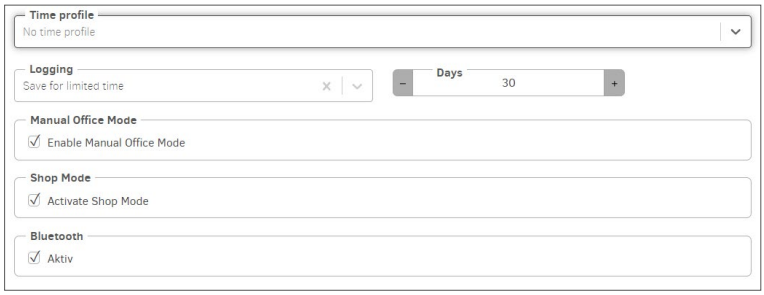
Logging:
definition of the access event recording type and the duration of data recording

Manual office mode:
manual office mode is active or inactive

Shop mode:
shop mode is active or inactive

Bluetooth:
for components with Bluetooth functionality, this can be activated or deactivated. Changes are made via maintenance tasks.

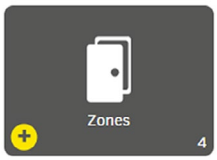
The component does not have to be removed from the system for this. The status of the component is displayed in the software after it has been added.



The **Office mode** is a time-controlled permanent opening of the access component. In the defined period – e.g. office hours or business opening hours – access is possible without authorisation.

The **Shop mode** is only started when an authorised access medium is held to an access component.

17.8 Areas



Access points can be merged into areas. This is useful if several access points have the same characteristics, e. g. the same authorisations, organisational affiliation, such as departments or building sections.

A maximum of 95 areas can be user-defined for each installation (partition).

The area Installation is automatically created when the system is created. It contains all access points and cannot be changed or deleted.

If this area is selected for an authorisation profile, then all access points are affected.

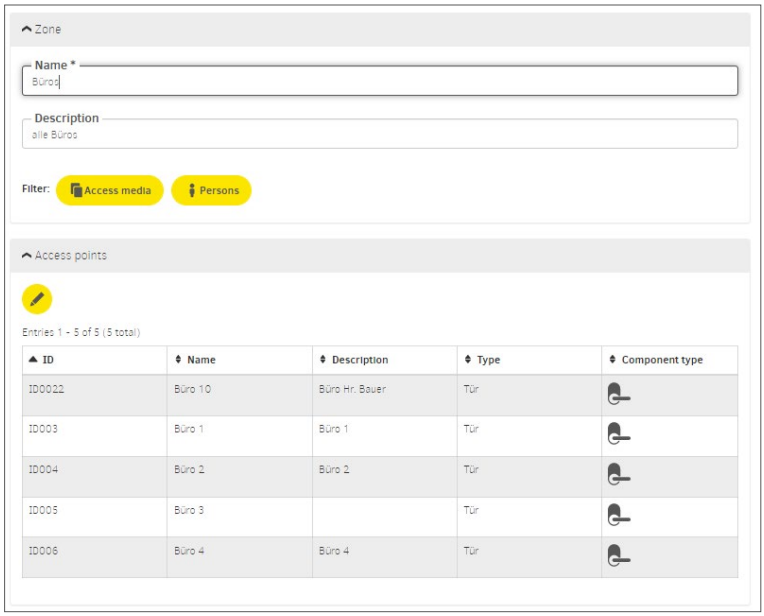
It is not possible to import a Xesar 2.2 system with 96 areas. Therefore, remove an area from the Xesar 2.2 system before importing.

Example – display office area:
Mandatory fields are marked with *.

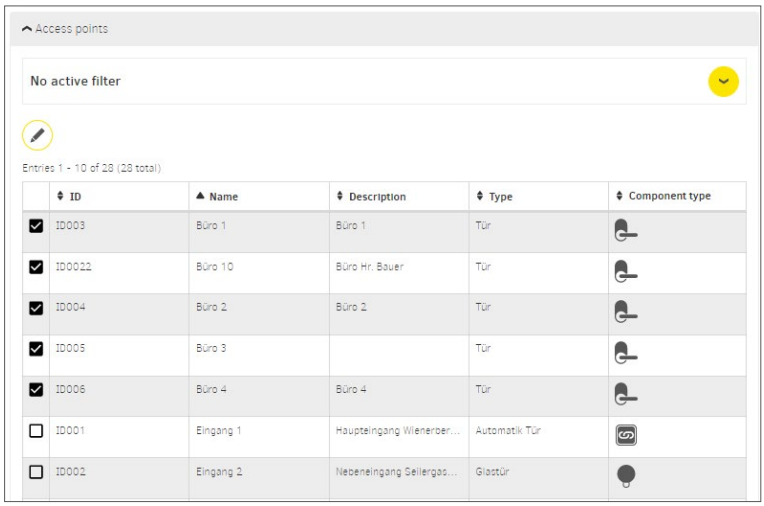
Name:
Name of the area

Description:
supplementary information relating to the name

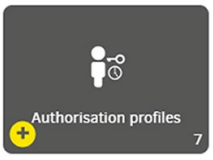
Access points:
shows the selected access points



Select access points:
select the access points for the area by ticking the box in the first column.



17.9 Authorisation profiles



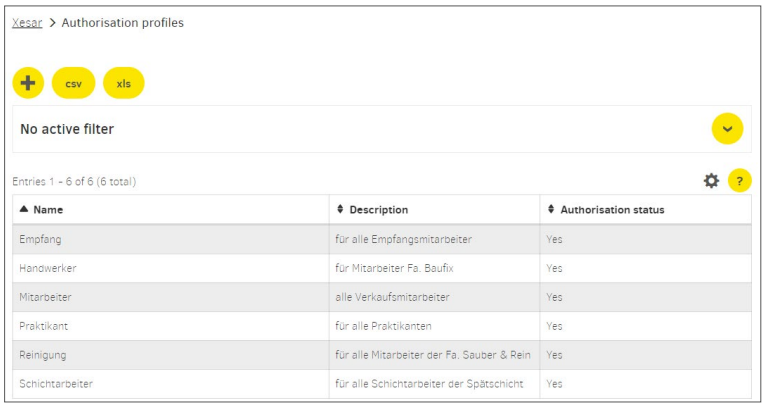
Authorisation profiles describe spatial and temporal access restrictions for access media. These access media can be assigned to persons. This means that a person with an access medium only has access to the access points and areas defined in the authorisation profile and only at the defined times. Access will be denied at other installation points and outside the defined times.

An authorisation profile can be assigned to many access media (e. g. all of the people in a department with the same authorisations).

Only one authorisation profile can be assigned to each access medium. In addition to this authorisation profile, a maximum of 3 individual authorisations for access points or areas with time profiles can be assigned to each access medium. (This is necessary, e. g. for access to lockers.)

If no access points or areas are assigned to an authorisation profile, the column **Status authorizations** in the overview list contains the entry**No**.

A maximum of 32 installation access points may be allocated to an authorisation profile.



Authorisation profile:

Mandatory fields are marked with *.

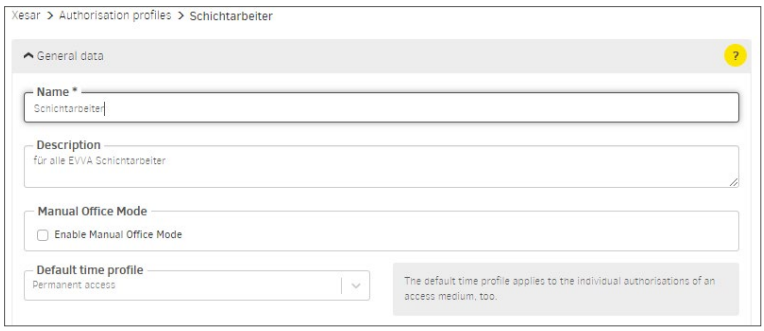
Name:
Name of the authorisation profile, e. g. shift worker

Description:
Additional information to the name, e. g. only for late-shift workers

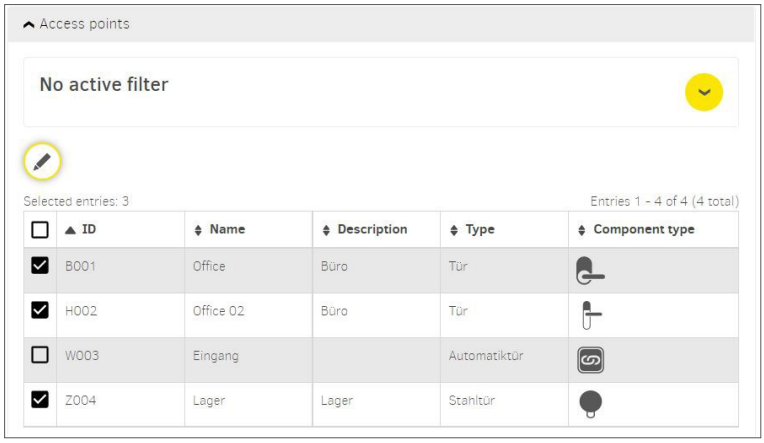
Manual office mode:
When Manual Office Mode is activated, all persons or access media have permission to activate Manual Office Mode on authorised access components.

Standard time profile:
Selection from the time profiles

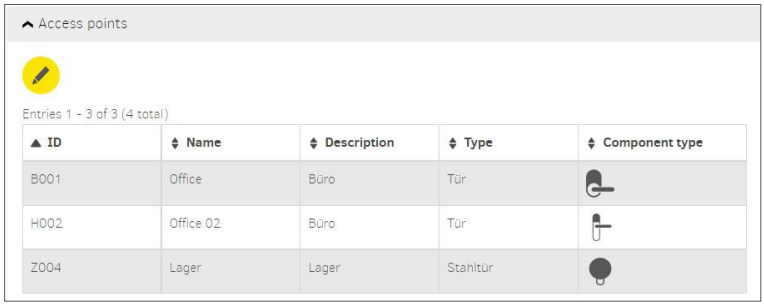
The standard time profile may only use time profiles with a maximum of 12 time slots.



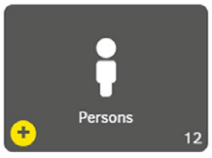
Selection of installation points:



Access to the selected access points:



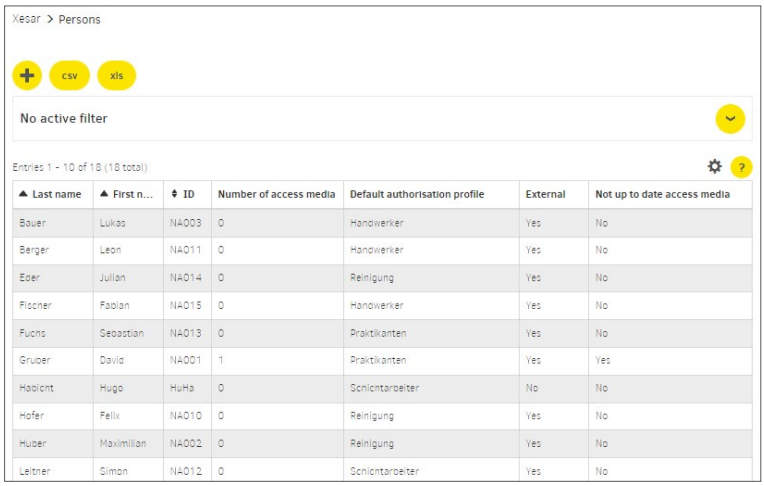
17.10 Persons



The "Persons" area defines all relevant information on the persons authorised in the installation. Persons in a installation can be assigned one or more access media with different authorisation profiles.

Persons can also be users with corresponding rights (according to the corresponding user group).

Display persons list:



Last name	First n...	ID	Number of access media	Default authorisation profile	External	Not up to date access media
Bauer	Lukas	NA003	0	Handwerker	Yes	No
Berger	Leon	NA011	0	Handwerker	Yes	No
Eder	Julian	NA014	0	Reinigung	Yes	No
Fischer	Fabian	NA015	0	Handwerker	Yes	No
Fuchs	Sebastian	NA013	0	Praktikanten	Yes	No
Gruber	David	NA001	1	Praktikanten	Yes	Yes
Habicht	Hugo	HuHa	0	Schichtarbeiter	No	No
Hofer	Felix	NA010	0	Reinigung	Yes	No
Huber	Maximilian	NA002	0	Reinigung	Yes	No
Leitner	Simon	NA012	0	Schichtarbeiter	Yes	No

Mandatory fields are marked with *.

First name:
The person's first name

Last name:
The person's last name

ID:
The abbreviation used for the person, e.g. initials

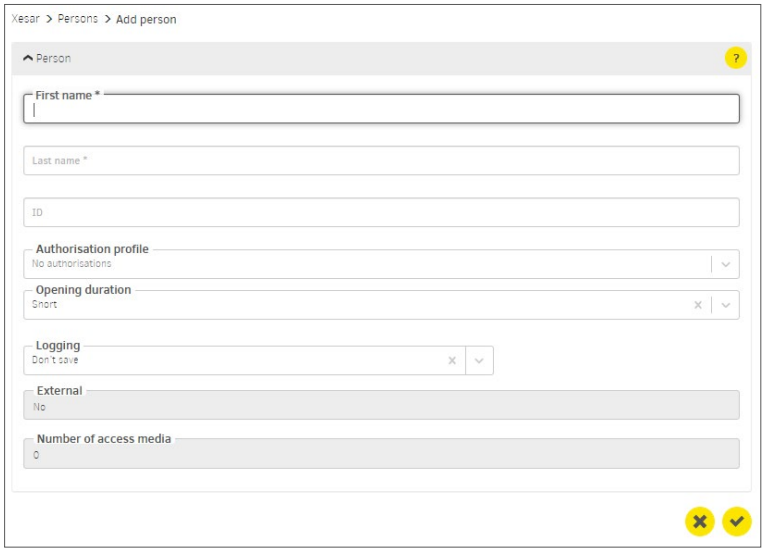
Number of access media:
The number of access media assigned to the person

Authorisation profile:
Selection from the authorisation profiles; is written to the access medium, which is assigned to the person, as the default authorisation profile.

External:
Yes – The personal data record is managed by a third-party system via the third-party system interface.
No – The personal data record is managed manually in the Xesar software

Not-current access media:
Yes – at least one of the person's access media is not up to date and must be updated by holding it to the Xesar online wall reader or placing it on the coding station. (The status tile **Non-current access media** is yellow on the dashboard.)
No – all of the person's access media are up to date; it is not necessary to hold the access media to the Xesar online wall reader or place on the coding station.

17.10.1 Adding a person



Mandatory fields are marked with *.

First name:
The person’s first name

Last name:
The person’s last name

ID:
The person’s abbreviation, e.g. initials

Authorisation profile:
Selection from the authorisation profiles; is written to the access medium assigned to the person as the standard authorisation profile.

Opening duration:
The opening duration **Short** or **Long** is activated on the access component if access is authorised.

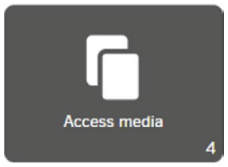
Logging:
Type of event recording - accesses can be recorded indefinitely or for a limited period.

Duration:
Enter the recording duration in days, if time-limited recording has been defined.

External:
Yes – The personal data record is managed by a third-party system via the third-party system interface.
No – The personal data record is managed manually in the Xesar software

Number of access media:
The number of access media assigned to the person

17.11 Access media

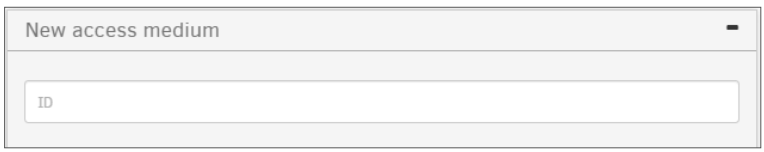


Access media are used to open doors using existing authorisation and to transfer system-specific security data between the access components and the management software via the XVN virtual network (Xesar virtual network).

In the Xesar access system, access media in the form of cards, key fobs, key cards, wristbands and stickers can be used as passive RFID media, as well as smartphone with BLE functionality.

17.11.1 New access media

When a new access medium is placed on the coding station, the following input field appears:



ID:
(Identifier or label is not a mandatory field)

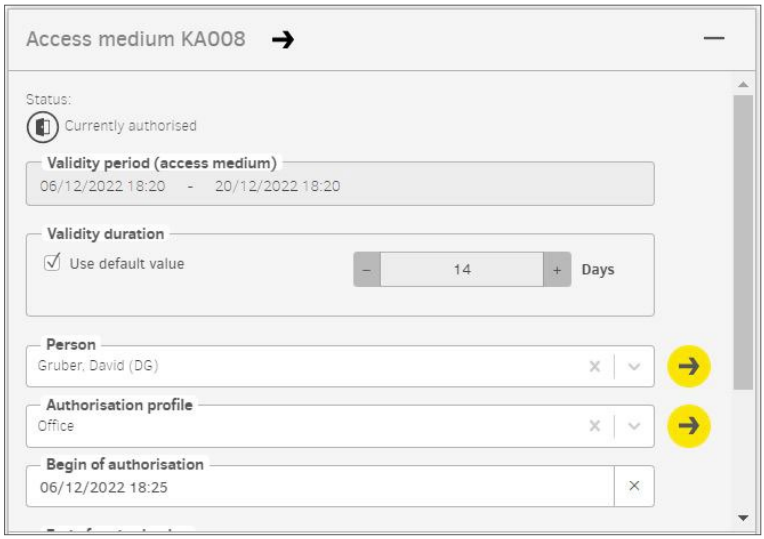
You can assign the access medium an access medium description (e.g. Hans Huber garage, visitor 1 or room 23).

An ID can be assigned or changed at any time in the detail view of the access medium in the Xesar software.

The label of an access medium is not anonymised when the accesses (personal reference) are not to be recorded. This means that the label should not include any personal reference, e.g. Hans Huber. This identifier is the responsibility of the user who issues the IDs for the access media.

In order for the ID of the access medium to be displayed in the event list, it must be assigned to a person. In the case of media with fire service or general master key authorisation, if it is not to be assigned to a specific person, a "fire service" or "general master key" person must be created and assigned accordingly.

After confirmation, another page appears with the following display and input fields:



Mandatory fields are marked with *.

Status:
Current status regarding validity and up-to-dateness.

Validity interval:
Selection of the time interval after which the access medium must be updated at the Xesar online wall reader or coding station (validity is extended).

Validity duration:
Information regarding the period for which the access medium is valid.

- **Default value:**
  is defined in the general security settings.

- **Individual:**
  Entry from 1 day up to max. 7300 days (approx. 20 years) and 1095 days (approx. 3 years) for smartphone.

Person:
The access medium can be assigned to a registered person. Several access media can be assigned to one person.

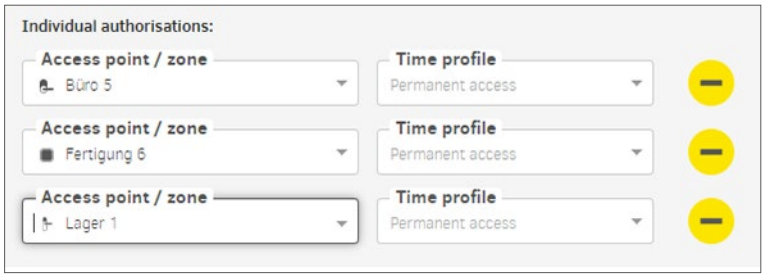
Access medium (substitute access medium) – The field only appears with a new access medium:
In order to create a replacement medium, the access medium to be replaced for the person selected above is selected here with his or her authorisation profile.

Authorisation profile:
Selection of the desired authorisation profile.

Begin of authorisation:
Point in time when authorisation of access medium begins. The time can also be in the future, e.g. for hotel bookings.

End of authorisation:
The time for the end of authorisation and validity of the access medium (e.g. end of work placement).
After this date, the validity of the access medium can no longer be extended.

Individual authorisations:
In addition to an authorisation profile, up to 3 additional individual authorisations can be assigned to an access medium.
Up to 3 access points or areas can be defined, each with a different time profile.
An individual authorisation does not have authorisation for manual permanent opening.



17.11.2 Add Smartphone as access medium

The following requirements must be met to open a Xesar system with a smartphone:

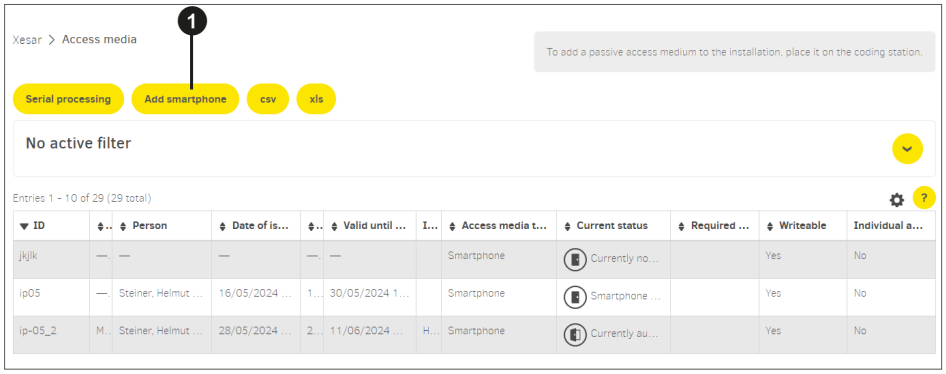
- Xesar software version 3.2 or higher is installed.

- Xesar components have Bluetooth function activated.
- Smartphone (iOS or Android) has Xesar app installed and authorised.

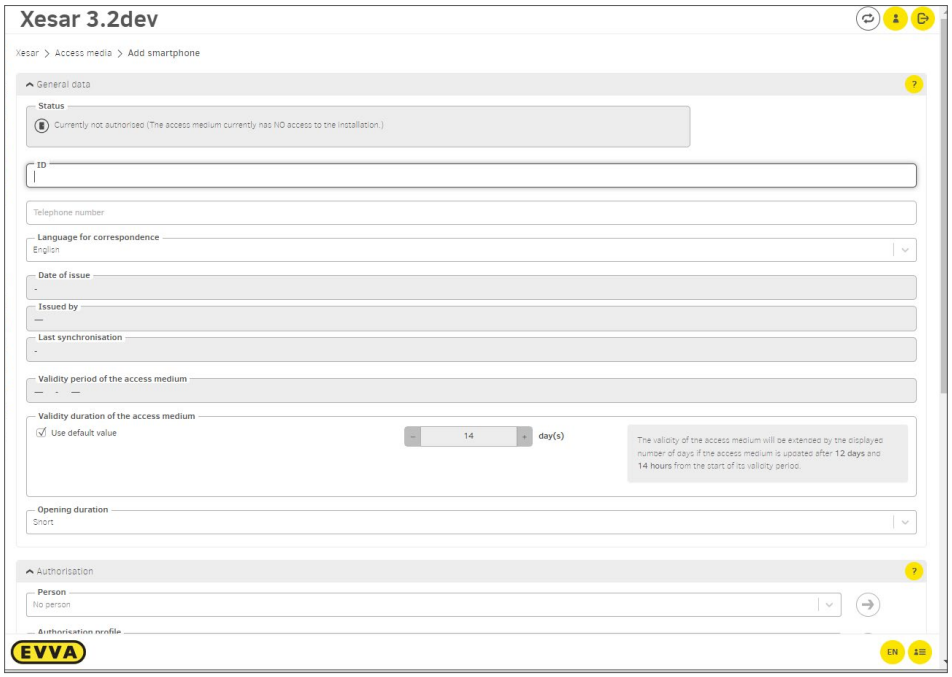
To register and for updates, the smartphone must be connected to the Xesar system via the Internet.

Here you can set the standard access authorisation for smartphone - but not for passive access media.

» Add a smartphone as an access medium.



» Press the **Add smartphone** button ❶ to open the details page.



General data:

Status:
Current status regarding validity and up-to-dateness.

ID:
(Identifier or label is not a mandatory
field). You can assign an access medium designation to the access medium (e.g. Hans Huber garage, visitor 1 or room 23). You can
assign or change an ID at any time in the access medium detail view in the Xesar software.

Telephone number:
Entry is only necessary if the registration code is to be sent by SMS (not a mandatory field).

The phone number of the smartphone must start with **+** and country code, and may contain max. 50 characters (+, 0–9 and spaces).

Correspondence language
Select the language of the standard SMS message sent to a smartphone.

Issue date:
Date of the first issue of the access medium.

Issued by:
Name of the user who issued the access medium.

Last synchronisation:
Time of the last update.

Validity interval of the access medium:
Displays the time interval until the access medium is updated again via XMS (Xesar Mobile Service). An Internet connection is required for this.

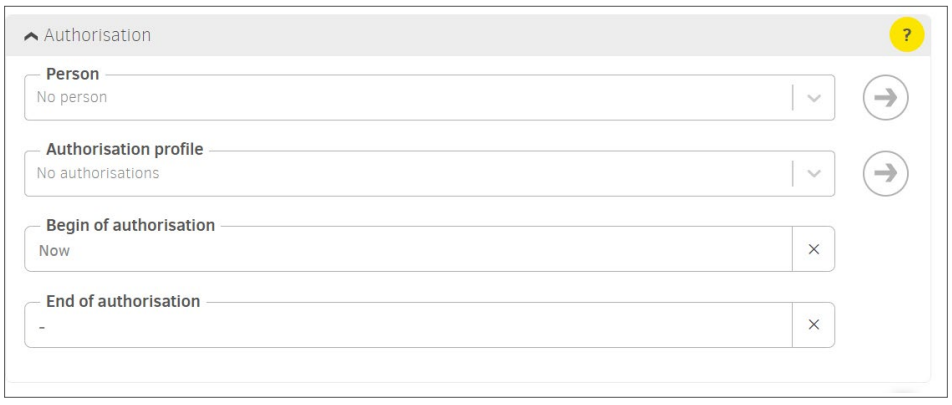
Validity duration:
Information regarding the period for which the access medium is valid.

Use default value:
This is defined in the general security settings under Default validity duration of a smartphone.

Individual:
Define the validity duration of the smartphone (from 1 to max. 1095 days = approx. 3 years).

Opening duration:
The opening duration defines the time during which the access component can be opened before it disengages (locks) again. The corresponding opening duration is "Short" or "Long". The opening duration is defined for the respective person or access medium and is triggered when authorisation is granted for the access component. The opening duration is assigned to the person or access medium in the person and access medium settings.

Authorisation:



Person:
The access medium can be assigned to a registered person.

Several access media can be assigned to a single person.

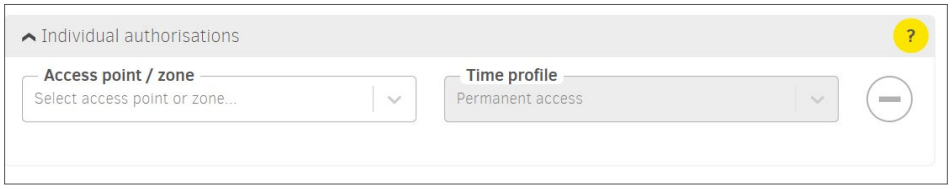
Authorisation profile:
Selection of the desired authorisation profile.

Authorisation begin:
Point in time when authorisation of access medium begins. The point in time can also be in the future, e.g. for hotel bookings.

End of authorisation:
The point in time at which the authorisation and validity of the access medium ends (e. g. completion of a work placement).
After this time, the validity of the access medium can no longer be extended.

The fire service authorisation profile is not applicable for smartphone.

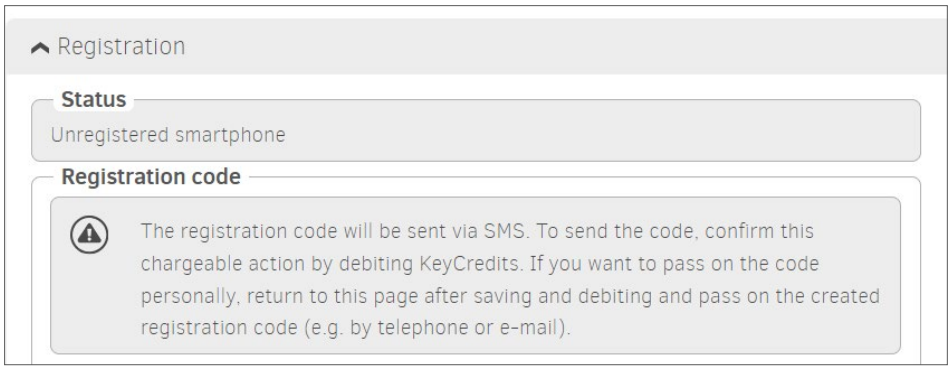
Individual authorisations:



In addition to an authorisation profile, up to 3 additional individual authorisations can be assigned to an access medium.

3 installation access points or areas can be defined with different time profiles.

Registration:



The smartphone is added to the installation with the registration. The registration code is generated after saving the entered data and sent by SMS to the specified telephone number. If no telephone number has been saved, the code can also be copied and sent to the smartphone by email. The code can also be transferred to the smartphone using a QR code.

If authorisation is granted at the same time as smartphone are added, KeyCredits are required for this promotion (unless a lifetime licence has been purchased).
Make sure that there is enough KeyCredits credit available.

The generated registration code is valid for 48 hours. If it is not used during this time, a new code can be generated and sent.

After successful entry of the registration code on the smartphone, the registration status changes to
"completed". If necessary, an output log can be created and handed over.

Change smartphone authorisations

Authorisation changes in the Xesar software and updates are automatically transferred over-the-air to the smartphone via the Xesar Mobile Service (XMS). This requires an active Internet connection.

Deleting smartphone authorisations

An active Internet connection is required.
All authorisations, including individual authorisations, are deleted on the smartphone.
The smartphone remains in the installation and can be authorised again.

No blacklist entry is generated.

Resend Permissions

An active Internet connection is required.
All authorisations are sent to the smartphone again.

Withdraw smartphone

An active Internet connection is required
When the smartphone is withdrawn, all authorisations are deleted.
No blacklist entry is generated

Block smartphone authorisations

The smartphone is blocked in the installation and a blacklist entry is generated. To guarantee the security of the installation, perform the blacklist distribution maintenance task.

If the smartphone is withdrawn or authorisations are cancelled, authorisations are only deleted after the transfer has taken place. This is not guaranteed if the smartphone is not physically present.
If the smartphone is offline or unreachable, it cannot be ensured that the authorisations have actually been withdrawn. If there is uncertainty about the whereabouts of the smartphone (e.g. if it has been lost), we recommend to deactivate the smartphone. (The smartphone should be deactivated directly by the system operator). A blacklist entry is generated) and maintenance tasks perform.

If the app on the smartphone is erroneously deleted, the authorisation can be sent to the smartphone again with “Generate new registration code”.

Smartphone or SIM card replacement

Access authorisations are generally stored in the Xesar app on the smartphone.

- Smartphone replacement
  The Xesar app must be deleted from the old smartphone. After updating via XMS, the status changes to “Smartphone no longer linked”. Install the Xesar app on the new smartphone. Now use “Generate new registration code” to register the new smartphone. The existing data is retained.

- SIM card or telephone number exchange: Access authorisations remain on the smartphone. No changes are necessary because the smartphone communicates with the Xesar system via XMS (Xesar Mobile Service) and not via a GSM network.

Observe the information on installing and operating the Xesar app on the smartphone (see chapter “Xesar app for smartphone”).

17.11.3 Existing access medium

After placing an existing access medium on the coding station (or for smartphone on the details page), the following input window is displayed:

Status of the access medium:

#	Status	Visualisation	Explanation
1	Insecure blocked access medium		There are still unsafe access points
2	Secure blocked access medium		There are no longer any unsafe access points
3	Unauthorised access medium		The access medium does not have any authorisation
4	Currently valid		
5	Currently invalid		
6	Currently valid access medium that becomes an invalid access medium when updated		
7	A currently invalid access medium that reverts to a valid access medium when it is updated		

#	Status	Visualisation	Explanation
8	Currently invalid access medium with a validity period on the access medium that lies in the future		
9	Deactivated (blocked) access medium		The access medium has been deactivated. There are no further unsafe access points and the calendar no longer plays a role

Validity period:
Selection of the period ending when the access medium must be updated again at the Xesar online wall reader or the coding station (validity extended).

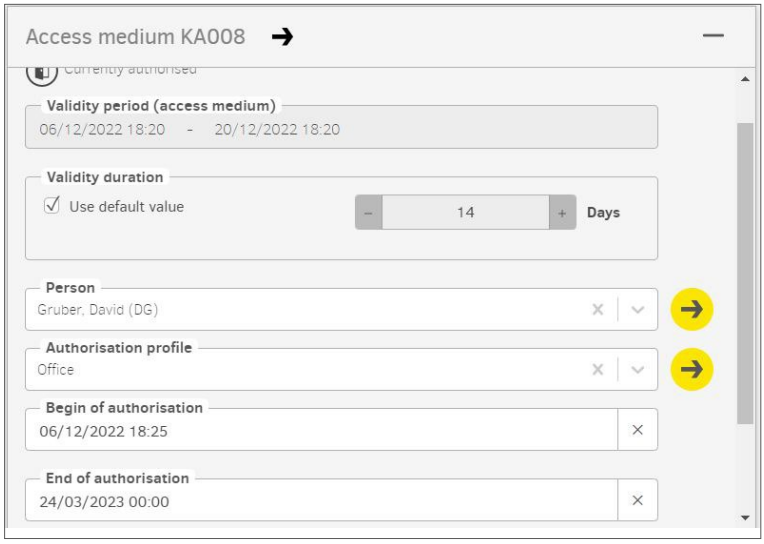
Validity duration:
Information regarding the period for which the access medium is valid.

- **Default value:**
  is defined in the general security settings.
- **Customised:**
  entry from 1 day to max. 7300 days (about 20 years).
  Smartphone: from 1 day to max. 1095 days (approx. 3 years).

Person:
Person to whom this access medium is assigned

Begin of authorisation:
Point in time when the access medium is valid or has update authorisation

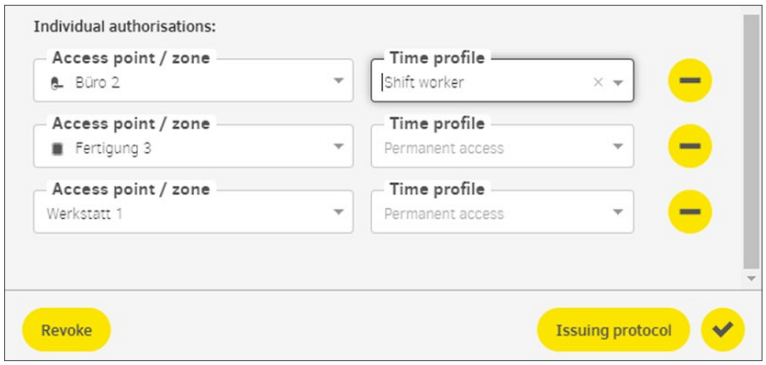
End of authorisation:
From this point in time, the access medium is no longer valid or authorised for authorisation updating



Individual authorisations:
Individual authorisations can be assigned to access media for 3 access points or areas (e.g. for a personal locker or garage space).

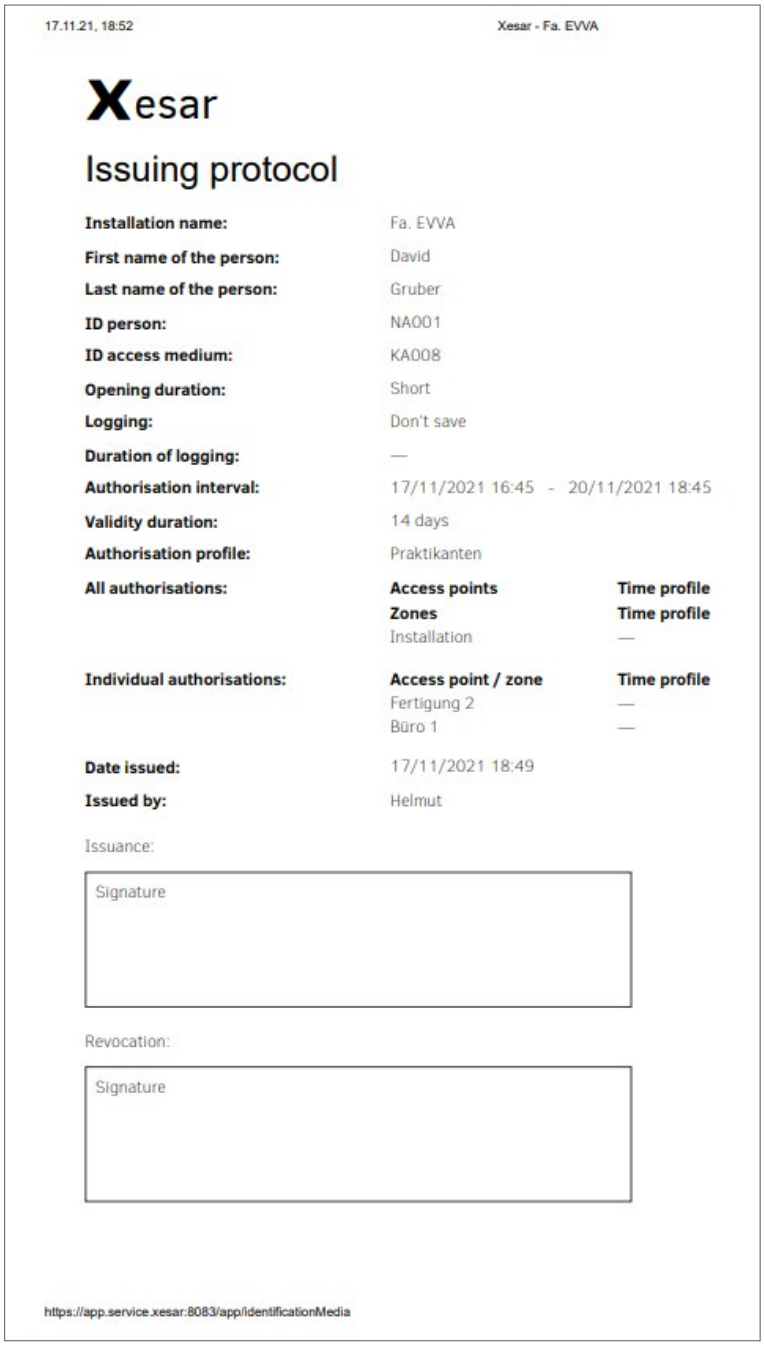
Withdraw:
Click on the **Withdraw** button to revoke the medium. All settings except the identification number are deleted. (The function is used, e.g. for access media of employees who leave the company)

Access media can be reused. Therefore, do not use personal data as part of the access media ID.



Output log:
Click on the **Output log** button to generate an access media output log with all relevant data in .pdf format. The pdf file can be printed out and signed by the recipient when they accept the access medium.

Create a new output log when authorisations are changed.



17.11.21, 18:52 Xesar - Fa. EVVA

Xesar

Issuing protocol

Installation name:	Fa. EVVA	
First name of the person:	David	
Last name of the person:	Gruber	
ID person:	NA001	
ID access medium:	KA008	
Opening duration:	Short	
Logging:	Don't save	
Duration of logging:	—	
Authorisation interval:	17/11/2021 16:45 - 20/11/2021 18:45	
Validity duration:	14 days	
Authorisation profile:	Praktikanten	
All authorisations:	**Access points**	**Time profile**
	Zones	**Time profile**
	Installation	—
Individual authorisations:	**Access point / zone**	**Time profile**
	Fertigung 2	—
	Büro 1	—
Date issued:	17/11/2021 18:49	
Issued by:	Helmut	

Issuance:

Signature

Revocation:

Signature

https://app.service.xesar:8083/app/identificationMedia

17.12 Add access components

When delivered, access components are in construction mode. The access component must be added to the system to function in the Xesar system.

After defining the access point in the Xesar software, the access component is ready to be added to the system.

▲ ID	Name	Description	Type	Compone...	Component status
ID001	Eingang 1	Haupteingang Wi...	Automatik Tür		Prepared for installation
ID002	Eingang 2	Nebeneingang Sei...	Glastür		Prepared for installation
ID003	Büro 1	Büro 1	Tür		Prepared for installation

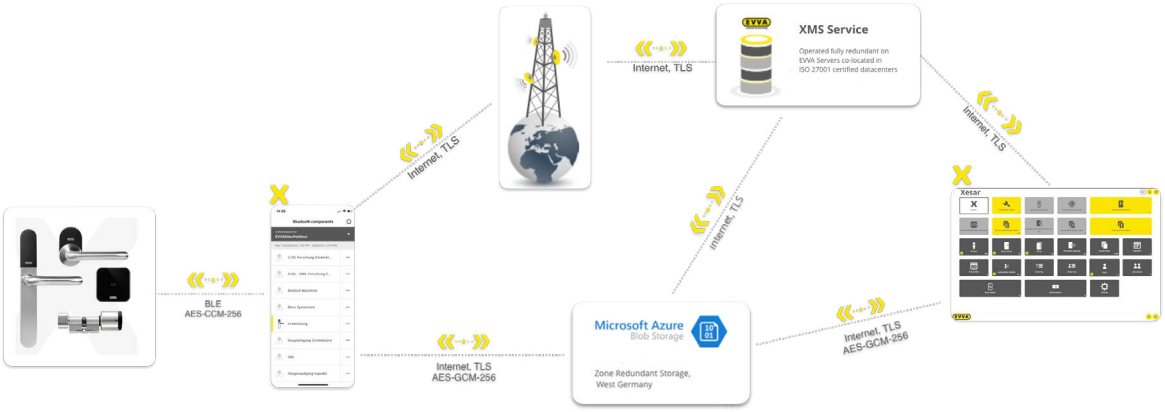
A configuration task is generated in the Xesar software to allow the addition of an access component.

This is synchronised to the Xesar tablet and, from Xesar 3.2, executed by the Xesar tablet using wireless synchronisation on the G2.1 access component. With older access components, synchronisation is performed using a connecting cable.

18 XMS – Xesar Mobile Service

Xesar Mobile Service (XMS) is an OTA (over-the-air) cloud service that enables secure communication between a smartphone and Xesar offline systems. Authorisations and their updates are sent via this connection. The Xesar system and the smartphone must be connected to the Internet. If one of the two components is offline, communication is delayed until the connection is re-established.

Communication is protected against misuse or manipulation by means of TLS encryption.



19 Xesar app for smartphones

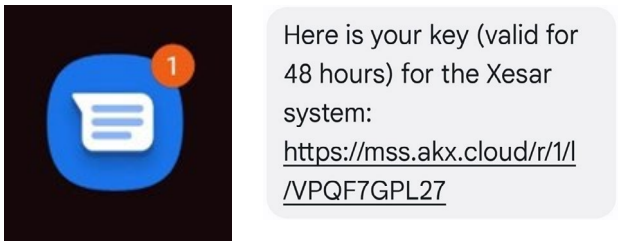
The Xesar app for smartphone with iOS or Android operating systems can be downloaded from the respective app store and installed.

To allow the smartphone to be used as an access medium in a Xesar installation, it must be added to the system and registered. (See chapter "Commissioning the Xesar software", adding a smartphone as an access medium.)

19.1 Xesar app installation

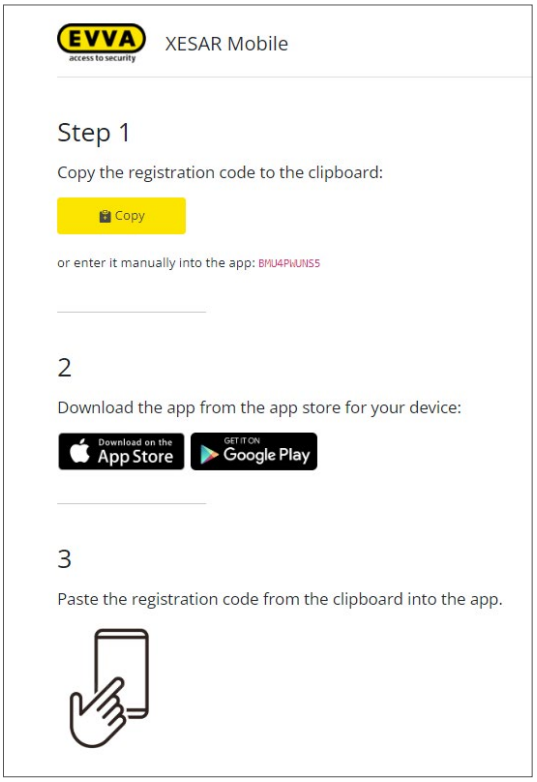
If the smartphone's telephone number is entered in the Xesar software during smartphone registration, an SMS message is sent to it. This SMS contains a link that leads to the registration code for the installation.

The sent link is valid for 48 hours. If not activated during this period, a new registration code must be generated and sent by the Xesar software.

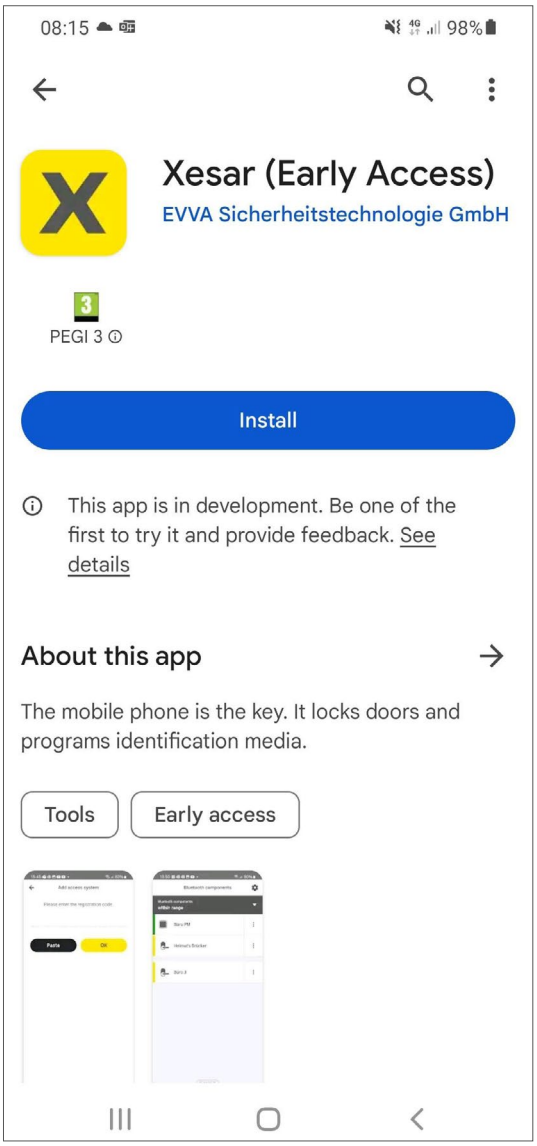


» Click on the link to go to the landing page.
Here you will find step-by-step instructions for installing and registering the Xesar app.

» Copy the registration code to the clipboard.

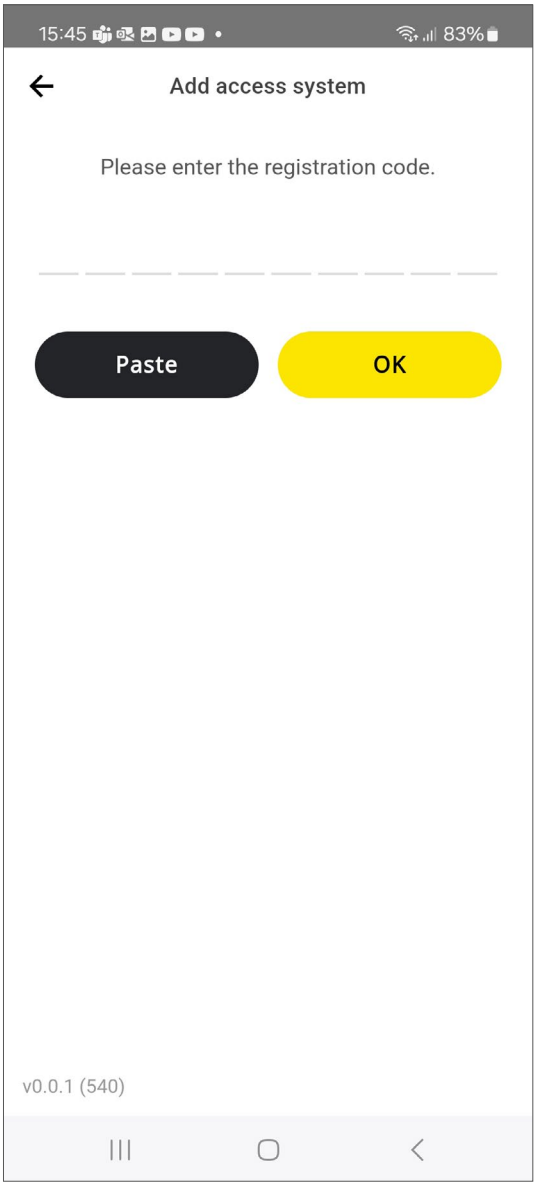


» Download and open the Xesar app from the app store.



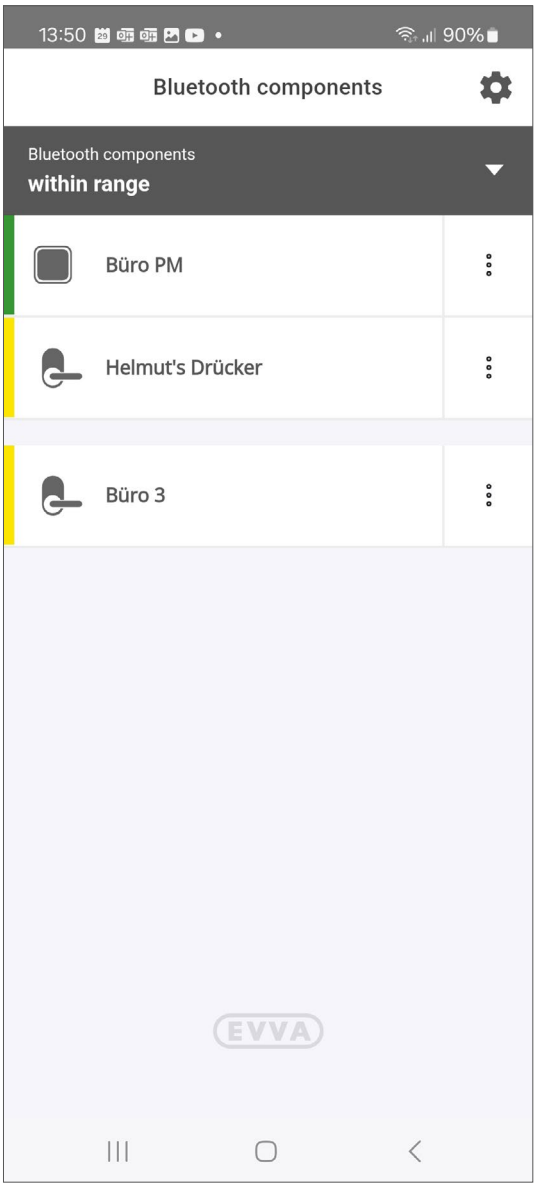
» Confirm the licence conditions and app authorisations.

» Add the registration code to the installation.



The Xesar app starts and scans for components within BLE range.

If an authorisation profile was also assigned when the smartphone was added, authorised installation access points within range will be displayed.

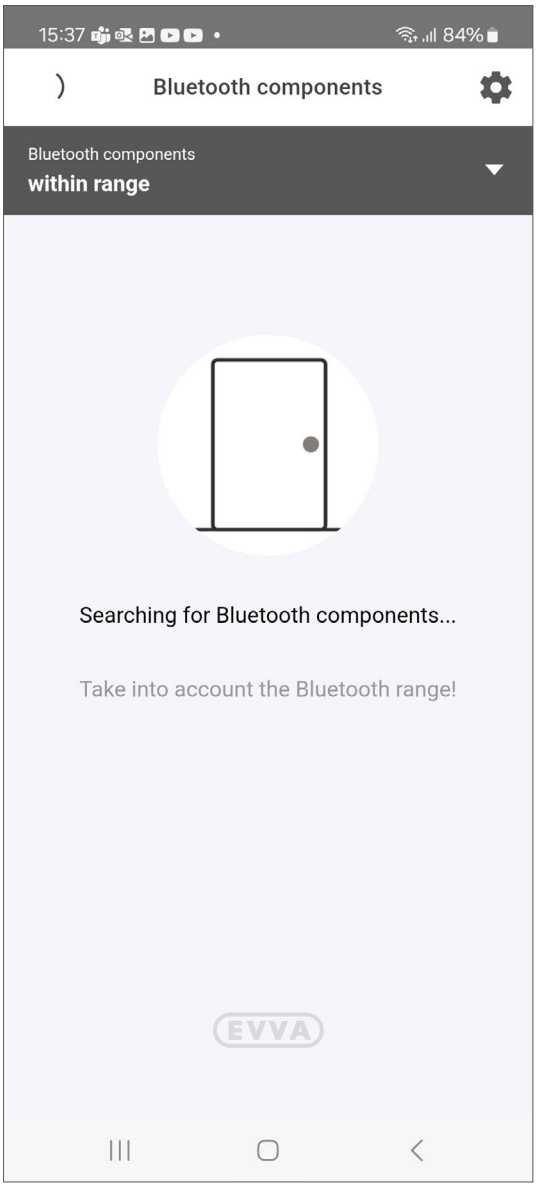


19.2 Xesar app operation

The Xesar app allows you to open installation access points of one or more Xesar systems with a smartphone, provided you are authorised to do so.

Furthermore, permanent opening can be activated and deactivated at defined installation points.

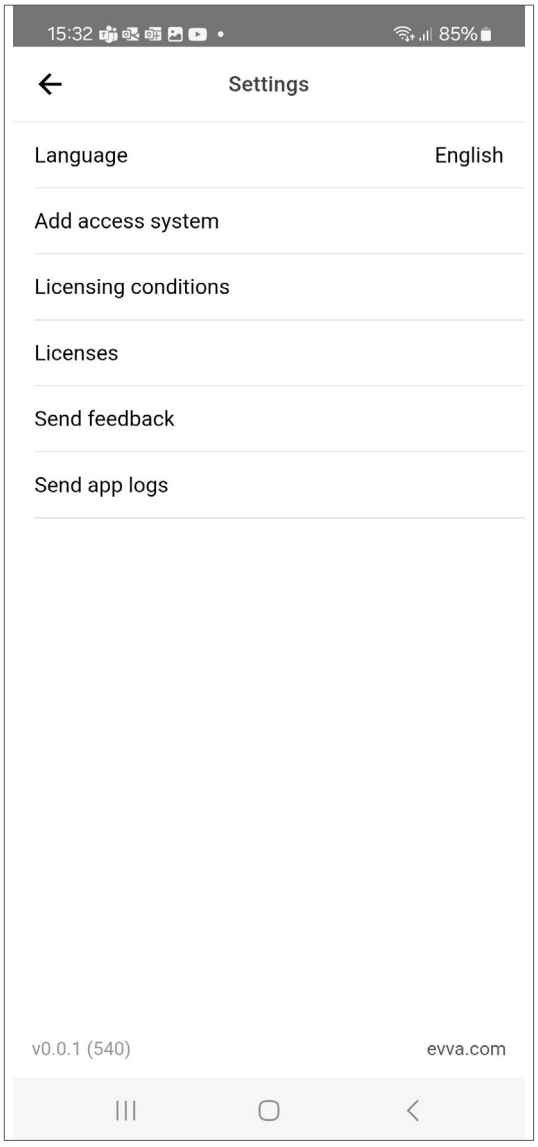
When you start the system or swipe down on the display to open it, the app automatically scans for authorised installation access points within range and displays
them. Non-authorised components of a system are not displayed.



19.3 Xesar app settings

» Click on the gear icon to open the settings page.

The following settings are available:



Language
App language setting options.

Add access systems:
Add additional Xesar systems (key ring function).

Licence conditions:
Display of EVVA licence conditions.

Licences
List of valid licences.

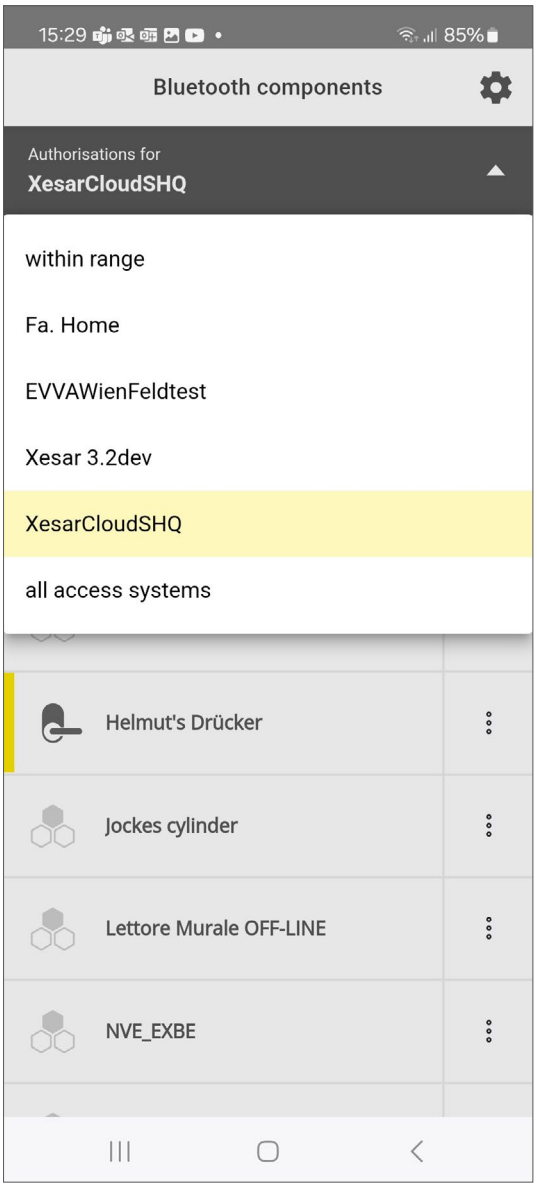
Send feedback:
Email link for sending feedback about the Xesar app to EVVA.

Send app logs:
Send app logs to EVVA if service is required.

19.4 Display of authorised Bluetooth components

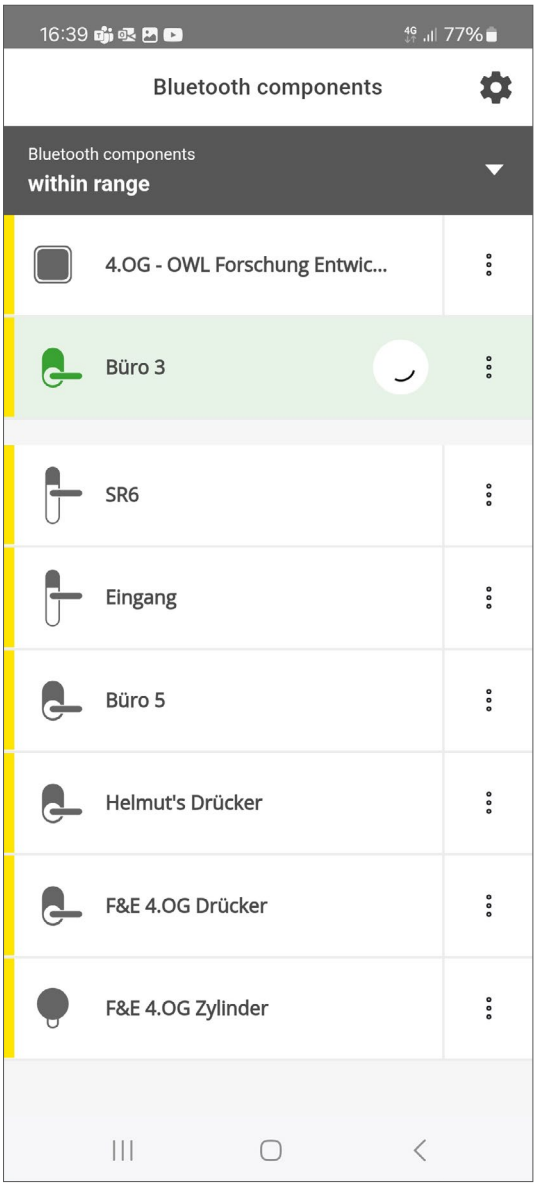
» Click on the down arrow to configure the display of authorised components.

- Within range
- Each access system (with individual authorisations)
- All access systems (with authorisations)



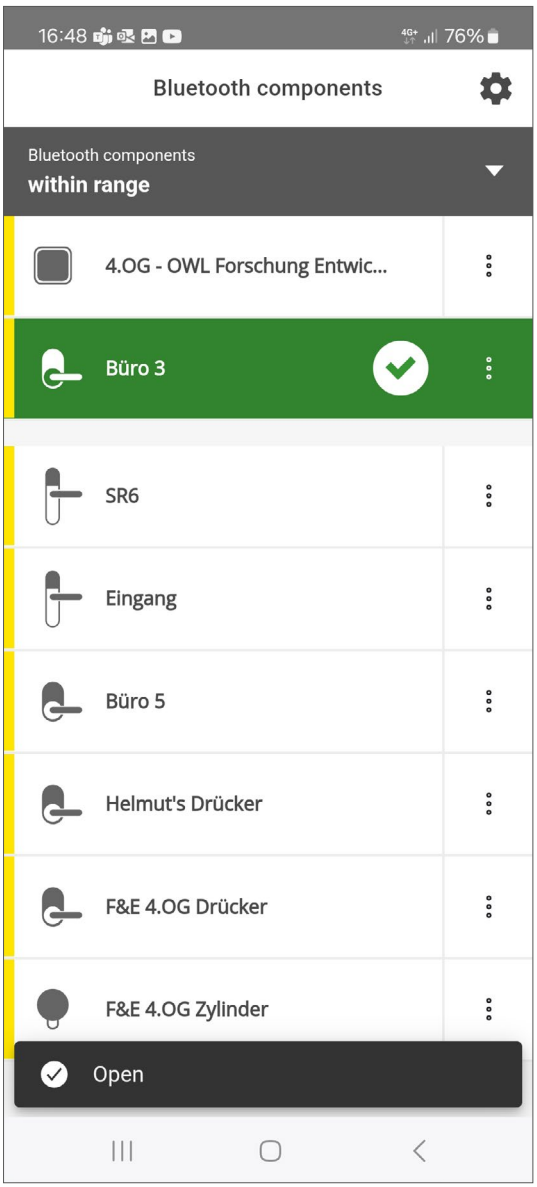
A neutral honeycomb icon is displayed when one or more authorised installation components are out of range. It is not possible to open them.

» Click on the component line to begin opening.



Depending on the BLE connection, opening may take a few seconds.

Successful opening is confirmed on the screen.

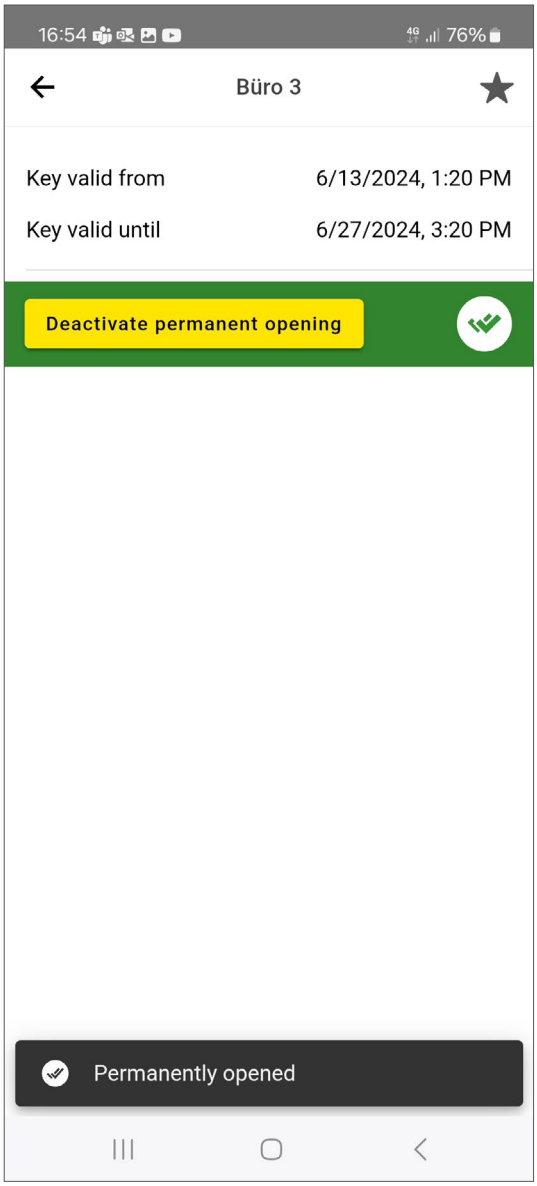


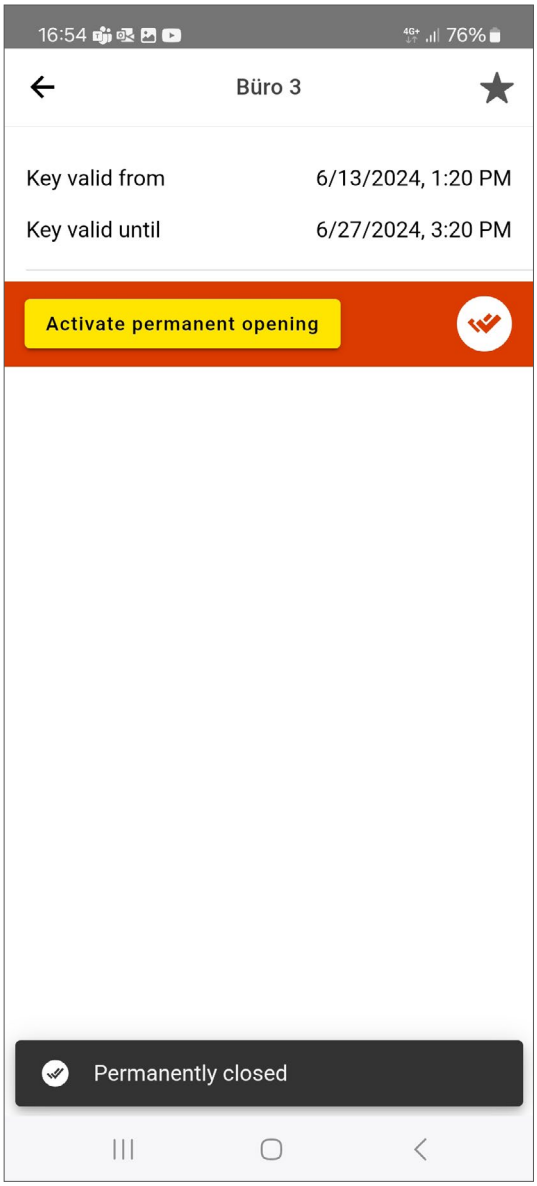
19.5 Activating and deactivating manual permanent opening (manual office mode)

» To access the manual permanent access point function, please click on the 3-point icon located next to the access point location to open the submenu.

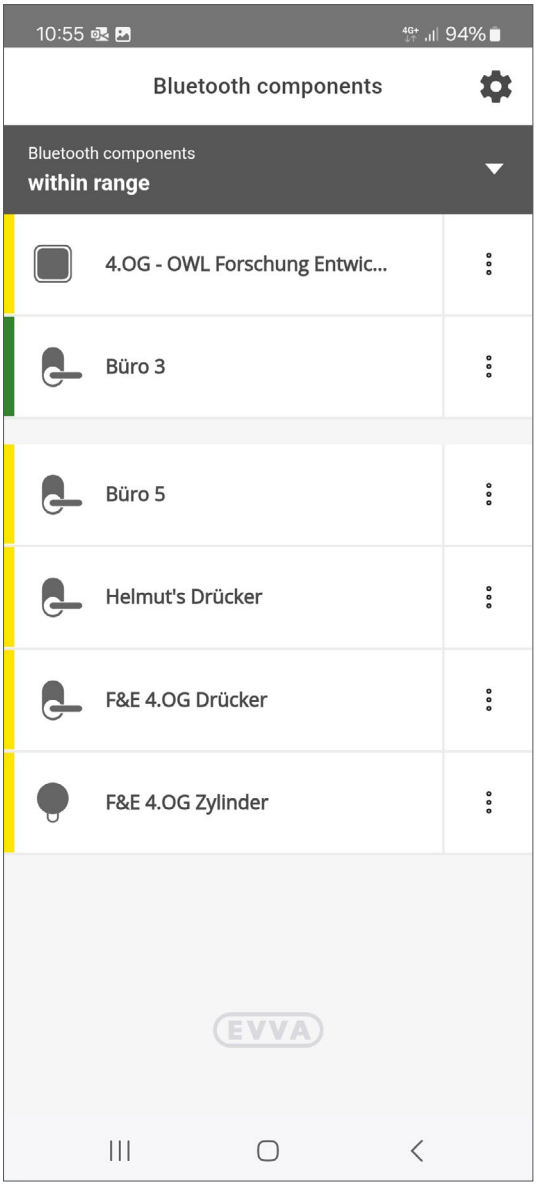
The **Manual Office Mode** function (permanent opening) is only available if the function is activated in both the authorisation profile used and the access point in the Xesar software.

» Click on the button **permanent opening activate /deactivate**, to change the respective status. If the component was permanently closed, it is switched to the permanently open state and vice versa.





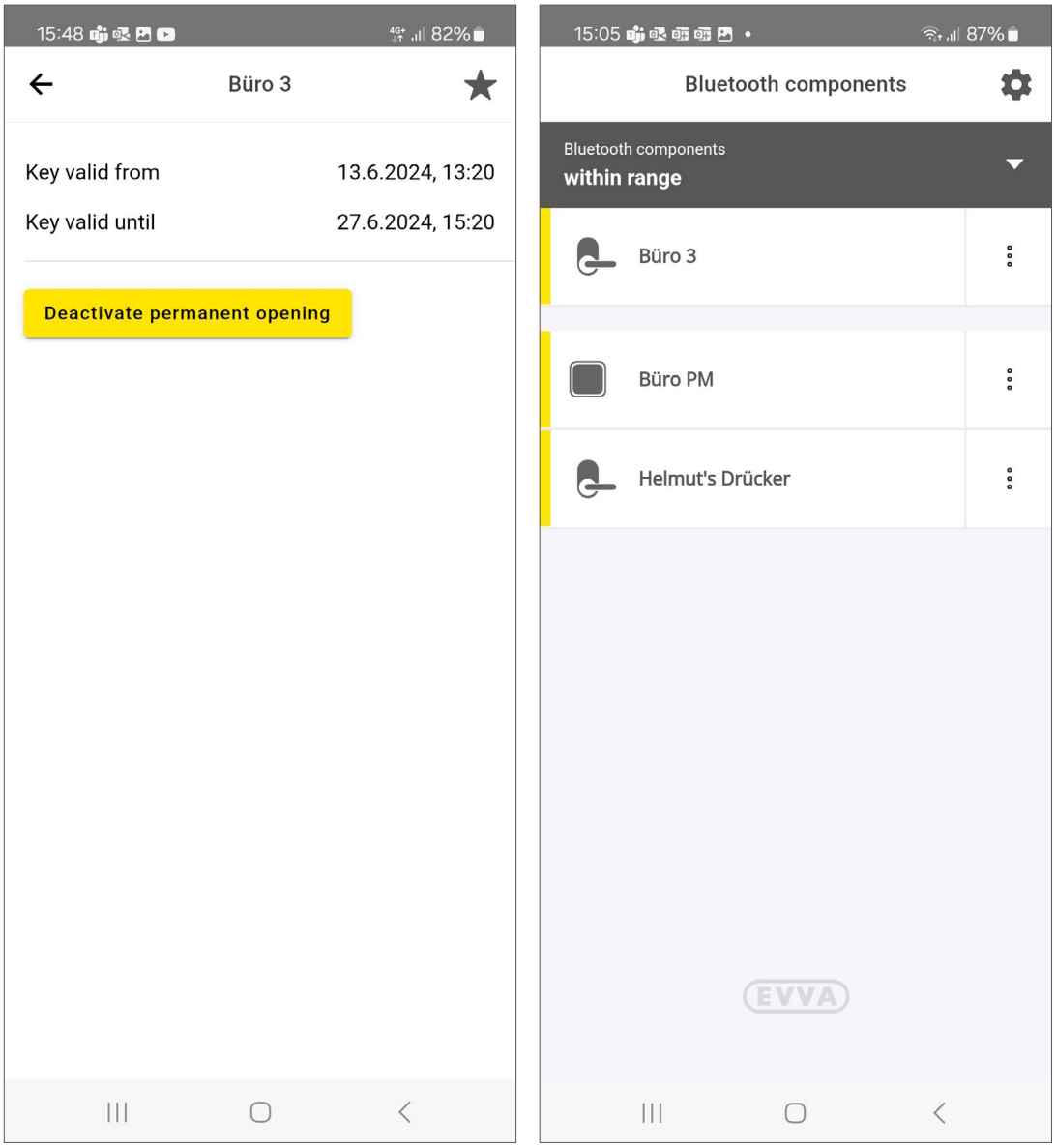
The message "Permanently open" is displayed when an access point is set permanently to open.
A green bar in the list also indicates the permanent opening of the access point.



19.6 Favourites display function

Installation access points that are frequently used can be marked as favourites by clicking on the star. They are displayed at the top of the “in range” view.

Several installation access points can also be marked as favourites.



20 Xesar system and installation management

Xesar software consists of the Installation Manager and other software applications such as Periphery Manager.

The Installation Manager installs and manages system-relevant Xesar system settings.

The Periphery Manager enables the connection and use of external components, such as the coding station.

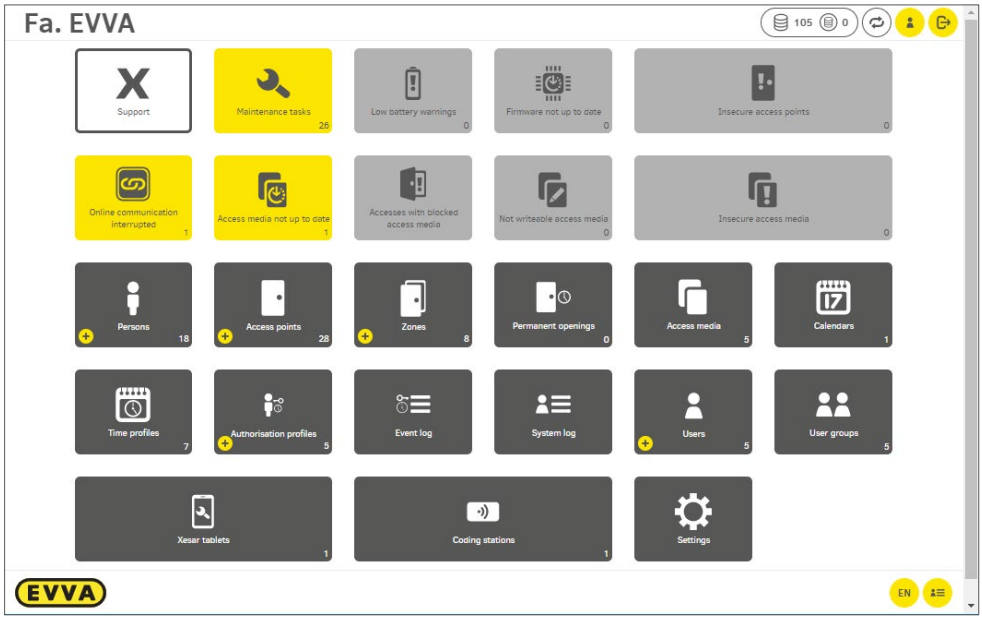
Xesar systems are managed on the management interface (dashboard) in the respective browser.

The dashboard provides an overview of the current security status of the Xesar system and the necessary maintenance tasks.

20.1 The dashboard

The Xesar dashboard provides a clear overview of Xesar functions.

The dashboard is the place to manage access media, users, doors, areas and authorisations. In addition, the dashboard displays warnings relating to insecure access media and access points, as well as maintenance task instructions (battery status and firmware status).



The dashboard is composed of tiles (fields) whose colour indicates various functions:

- Dark grey tiles are used for management purposes, such as the creation of areas, access points or authorisation profiles.
- Light grey tiles mean that no actions need to be set.
- Yellow tiles indicate warnings or instructions. As soon as the associated tasks are resolved, the tiles will become light grey again.
- The white support tile contains useful downloads, such as documents (e.g. the system manual) or files for exchange with the EVVA Technical Office in your country.

20.2 The list filter function

For detailed evaluation or for a simplified presentation, lists are filtered according to one or more criteria.

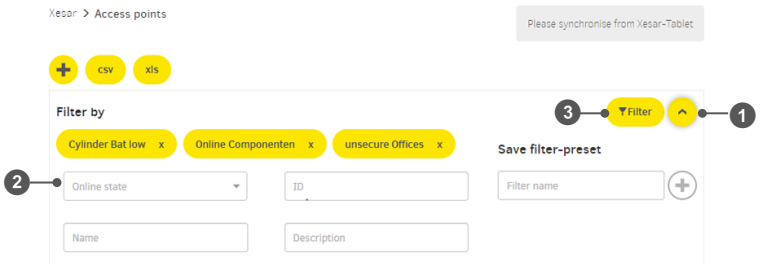
Filter settings that you need frequently can be saved as presets.

20.2.1 Manual filter

» Click on the **Open filter area** ❶ symbol

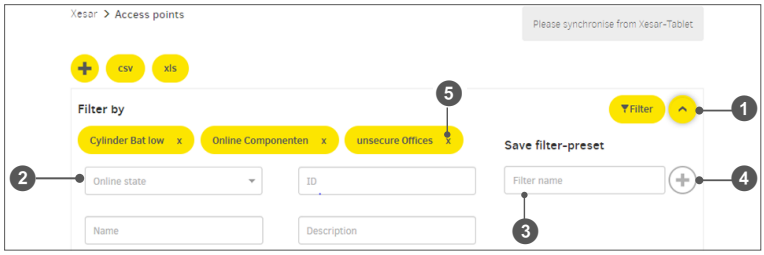
» Select the desired filter criteria ❷

» Click on **Filter** ❸



20.2.2 Filter presets

- Click on the **Open filter area** ❶ symbol
- Select the desired filter criteria ❷
- Assign a name for your filter preset ❸
- Click on the **Add** ❹ symbol
- Click on the **x** ❺ symbol in the button field to delete a filter preset.



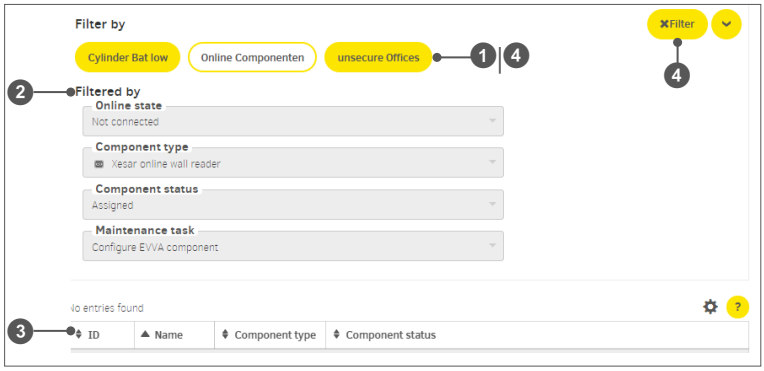
Apply filter preset:

- Click on the button to activate **Filter preset** ❶ | ❹

The filter criteria ❷ are displayed

The filter results ❸ are displayed in the list

- Click on the filter preset button again ❶ | ❹ or on the **Filter** ❹ button to exit the filter function.



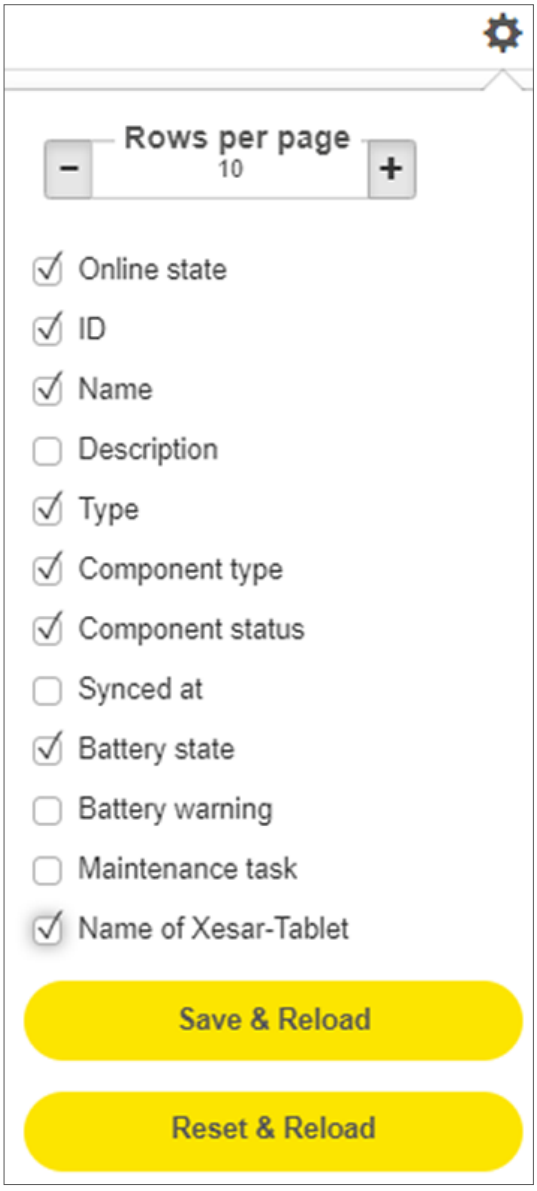
The number of filter presets per list is not limited.

20.2.3 Column view

The list view can be customised according to needs and the size of the display.

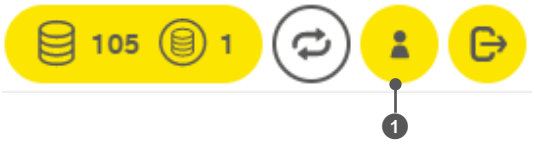
» Click on the ⚙ symbol to open the window to select the columns to be shown and hidden. In addition, set the maximum number of lines to be displayed per page in the selection window.

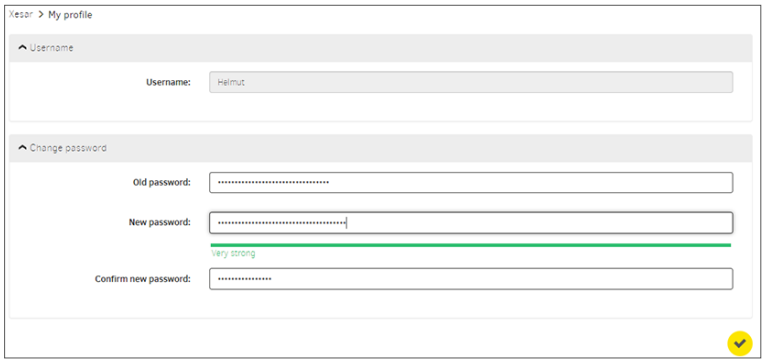
The settings made can be saved or re-set. The saved settings are retained for each individual user for all lists – even after leaving the page



20.3 My profile

The **My profile** ❶ menu item is located in the upper right corner of the dashboard. (Alternatively, you can access the **My profile** page via the **User** field and by selecting the user account.)





My profile directly provides information about which user is currently logged in (user name) and is managing the system.

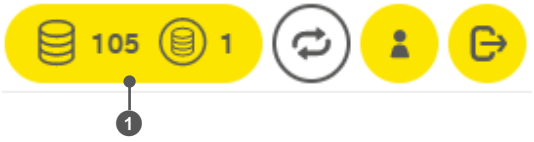
Changes to the user name and password can be made in the **My profile** area. When a password is changed, an evaluation of the security level of the password is automatically displayed. The spectrum ranges from very weak (red) to very strong (green).

20.4 KeyCredits (units)

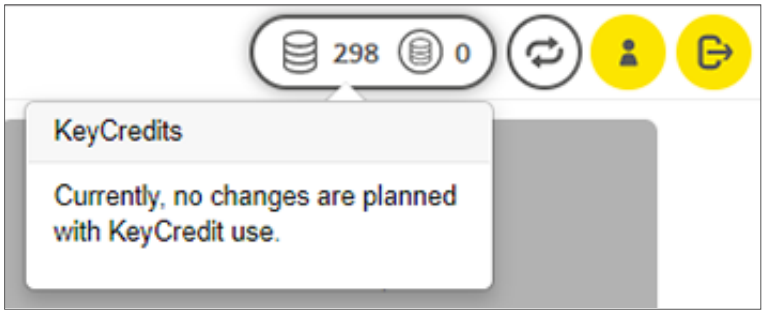
The dashboard displays the current credit balance and KeyCredits to be deducted ❶.

Chargeable changes are

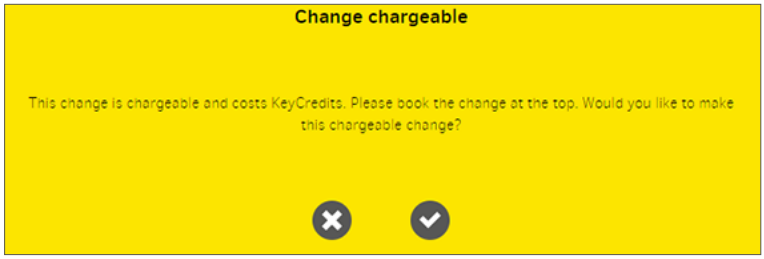
- Reissuing access media
- Changing authorisations



Blocking or withdrawing authorisations is free of charge.

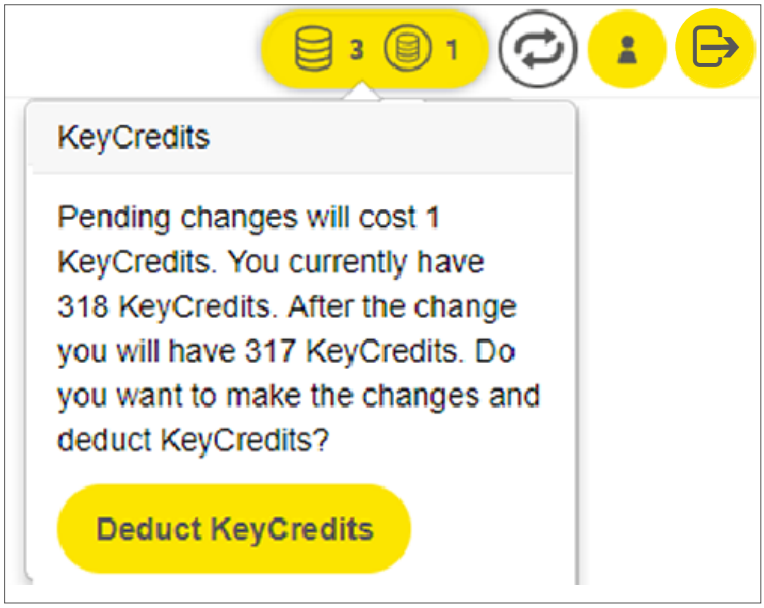


Chargeable changes are directly shown on the access medium when you create or change authorisations.



» Acknowledge the messages.
You can make further authorisation changes, and conclude by confirming the KeyCredits deduction.

The information about your KeyCredits is displayed on the dashboard.

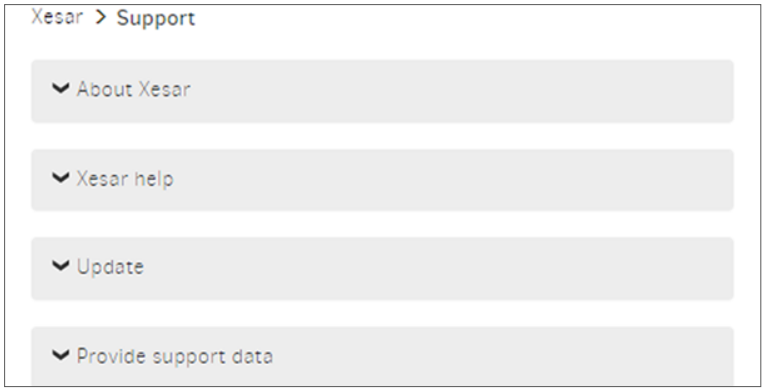


With KeyCredit Xesar lifetime, all changes to authorisations and issuing access media are included and do not need to be confirmed.

Note the information on recharging KeyCredits in the chapter “Installation Manager”.

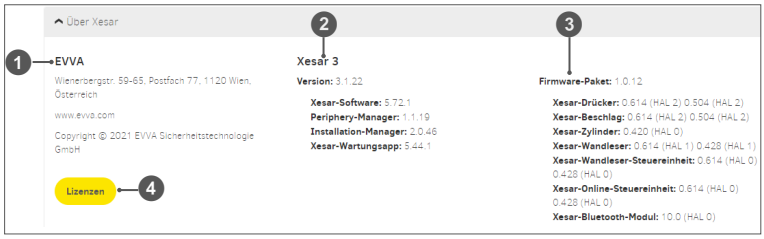
20.5 Support

The following support options are available on support page:



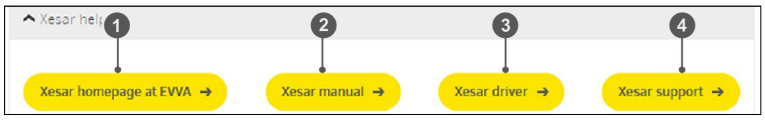
20.5.1 About Xesar

- EVVA company information ❶
- Installed Xesar version with the versions of the Installation Manager, Periphery Manager and Xesar maintenance app ❷
- Supplied firmware versions of the access components ❸
- Link to the EVVA General Licence Terms (with download option) ❹



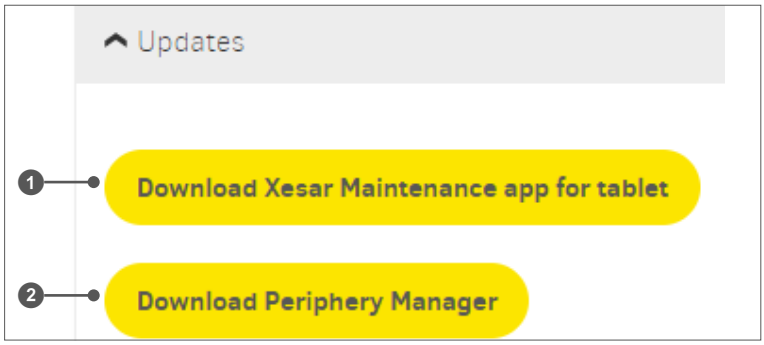
20.5.2 Xesar help

- Link to the Xesar product page on the EVVA website ❶
- Link to the Xesar system manual on the Xesar product download page ❷
- Link to the Xesar product page with information on downloading drivers for the coding station ❸
- Link to the Xesar EVVA support page ❹



20.5.3 Updates

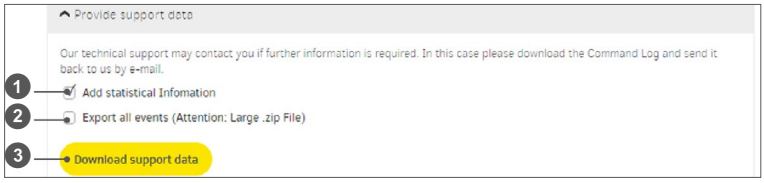
- Download the current Xesar maintenance app ❶
- Download the current Periphery Manager ❷



20.5.4 Downloading support information

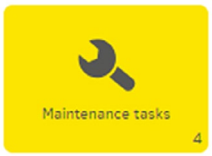
You can determine which support information is compiled.

- Include statistical information (for example, number of access points, areas, persons, identification media, blocked access media or access points per area) ❶
- All events or a limited number of events ❷
- Download the support information ❸



Download the support information as required. The anonymised system data is required for fault analysis. After consultation, send the data to the EVVA Technical Office.

21 Maintenance and configuration tasks



Maintenance tasks are configuration and maintenance jobs for access components, such as

- Adding
- Configuring
- Firmware update
- Removal

The **Maintenance tasks** tile changes to yellow when a new task has been added. It is automatically created by the system as soon as it is necessary to service an access component.

Maintenance tasks are carried out on access components using the Xesar tablet!

The user with the appropriate user group authorisation can synchronise maintenance tasks using the Xesar tablet (all tasks or by area). For this, access authorisation to the access points is not needed.

However, from a technical point of view, it is advantageous when the service technician has the access authorisation for the access points concerned. For this, he must be given an access medium with the appropriate access authorisations.

Software updates can also be performed when there are open maintenance tasks.
(No maintenance tasks may be open when upgrading from Xesar 2.2 to Xesar 3.x.)

21.1 Firmware update

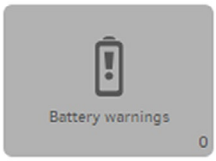
The **Firmware is not up to date** tile is light grey if no tasks are open. Where applicable, it becomes yellow and indicates the access components for which the firmware is to be updated. Updating the firmware offers the following advantages:

- Potential errors have been eliminated
- Battery service life increased by adjustments
- New functions added

A maintenance task is automatically created if an access component does not have the latest firmware.

You can also update the firmware without adding an access component to the system.

21.2 Battery warning



The **Battery warning** tile becomes yellow indicating all the access components for which the battery is empty and in need of replacement.

If the battery voltage of a component falls below the defined value, the information message “Empty battery” is triggered in the component and indicated by an optical and acoustic signal.

After the battery warning is displayed on the component for the first time, up to 1000 openings are still possible.

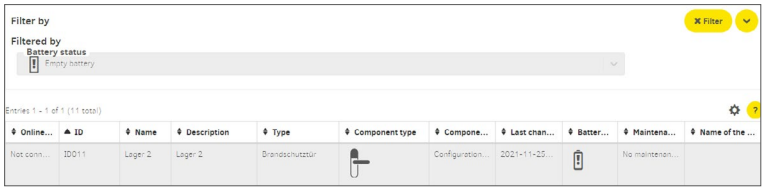
The information message “Empty battery” is transferred to the software using XVN via the media or the Xesar tablet. On the dashboard, the “Battery warning” is dis-

played on the yellow “Battery warnings” tile. Clicking on the yellow tile displays all components with a battery warning.

» Execute the maintenance task and
» replace the batteries as soon as possible.

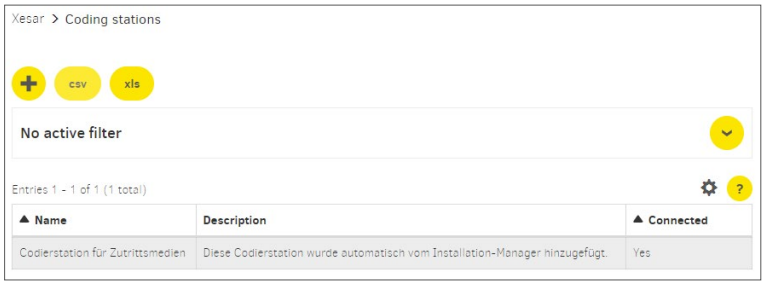
After replacing the battery, connect the component to the Xesar tablet and synchronise the Xesar tablet with the software. This will reset the battery warning in the software.

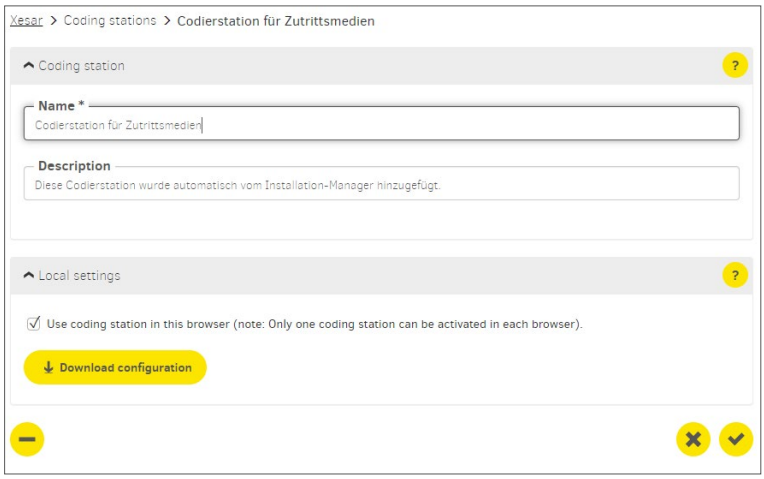
A maintenance task is created for all affected access components.



21.3 Coding stations

All active and inactive coding stations in use are listed in the **Coding stations tile**.





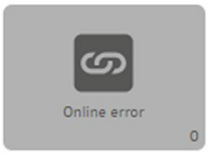
When installing PC systems, the coding station of the admin PC is automatically added by the Installation Manager. The coding station on the admin PC is managed via the system's configuration page in the Installation Manager. See chapter "Xesar installation".

To connect coding stations to client PCs, the Periphery Manager must be installed on the client PC.

An active coding station is required to issue or update access media.

Install and configure the Periphery Manager to connect the Xesar software and your system to the coding station. (See chapter "Link the coding station to the Xesar software".)

21.4 Online error

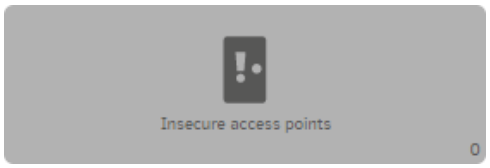


The **Online error** tile becomes yellow when an online error occurs. If the online wall reader has not been linked to the Xesar software, you will be unable to update access media on this online wall reader. However, the wall reader will function like an offline wall reader.

Please check if

- your Xesar network adapter is configured correctly
- the Xesar control unit is properly connected to the Xesar network adapter

21.4.1 Insecure access points

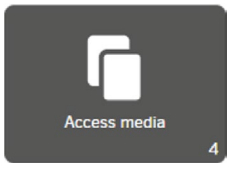


The **Insecure access points** tile becomes yellow if an access medium has been blocked and the blacklist at the access points is not up to date.

The blacklist update can be performed by the XVN or by a synchronisation between Xesar software and access component with the Xesar tablet.

A maintenance task is automatically created as soon as there is an insecure access point within the system.

21.5 Access media

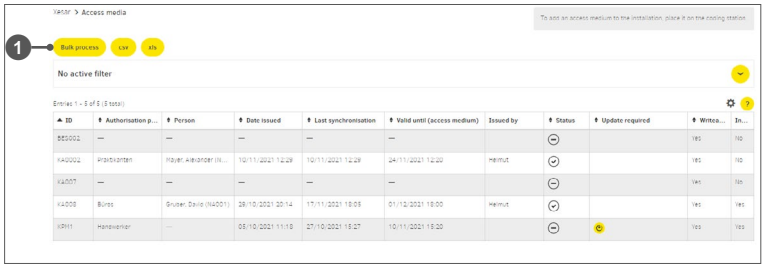


Different types of access media are available for Xesar (see chapter "Access media").

The number of access media displayed is the number of all access media in the system, regardless of whether blocked or blank. Access media cannot be deleted from the list.

21.5.1 Access media – batch processing

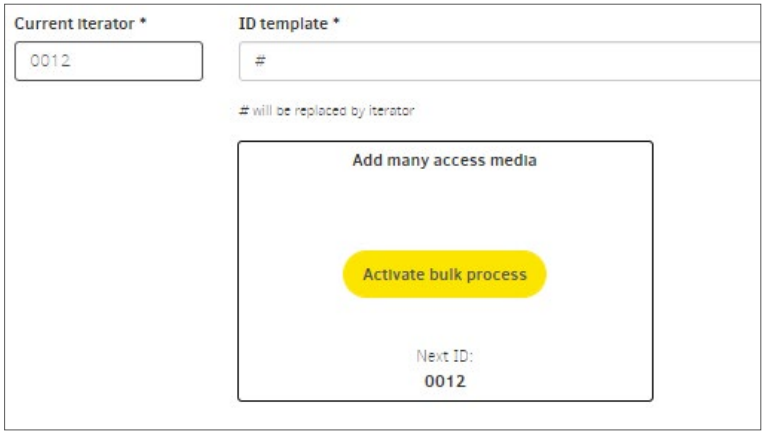
Xesar's batch processing function allows you to quickly and easily add several access media to the Xesar system. The batch processing function is available in the Access media tile in the **batch process** ❶ menu item



To begin batch processing, enter the latest serial number to assign a serial number to the access media in the Xesar software. If you do not assign a number, the Xesar system uses the default value and assigns the numbers automatically.

» Click on **Activate batch process** and place the first access medium on the coding station.

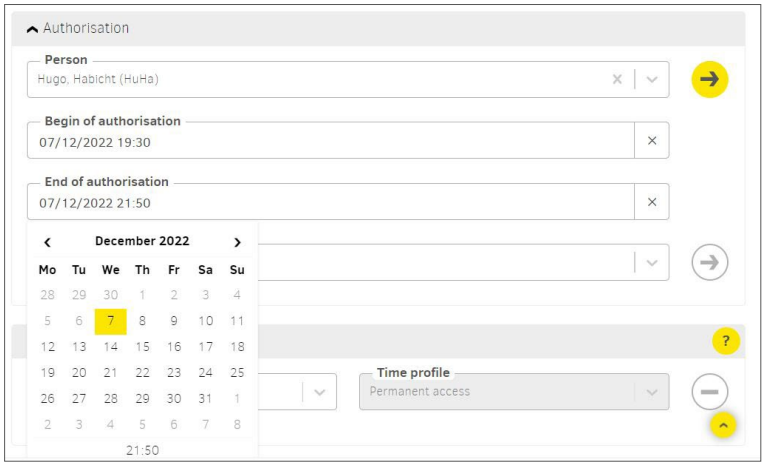
ID is e.g. the staff number.



Click on **Deactivate batch process** to stop batch processing.

21.5.2 Deactivate access media

The access medium can be deactivated if a person's access authorisation is to be suspended for an extended period of time. The medium with the authorisation profile remains allocated to the person. Access is deactivated until further notice by setting the end of authorisation to the current time.

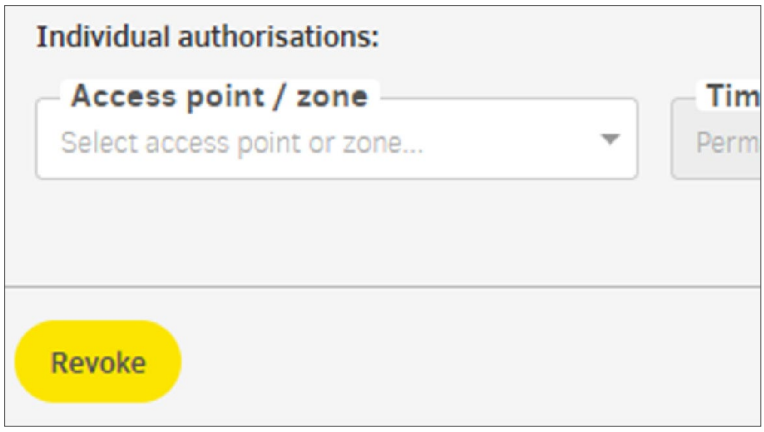


- Open the detail page of the access medium to be deactivated.
- Click on the current authorisation end date (date and time, e.g. 7.12. at 21:35). The medium is immediately deactivated.
- Then update the medium at the online wall reader or coding station so that it no longer has access to the system.

The access authorisation can be reactivated on the medium by setting a new authorisation end time and then updating it at the online wall reader or at the coding station.

No blacklist entries are generated in the system during this process.

21.5.3 Withdrawing access media



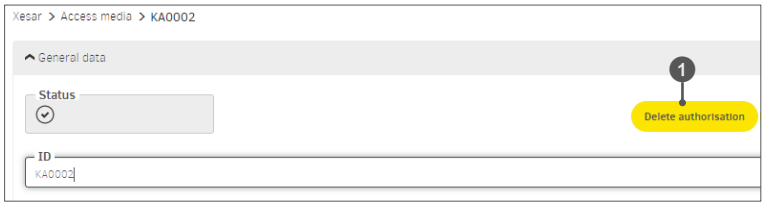
An access medium can only be withdrawn when it is positioned on the coding station. Only then is the **Withdraw** button visible. As part of this process, the saved data on the access medium is deleted and data can once again be written to the access medium.

The access medium remains in the list of access media.

Withdrawing an access medium deletes all data except for the installation key in the memory.

21.5.4 Deleting access medium authorisation

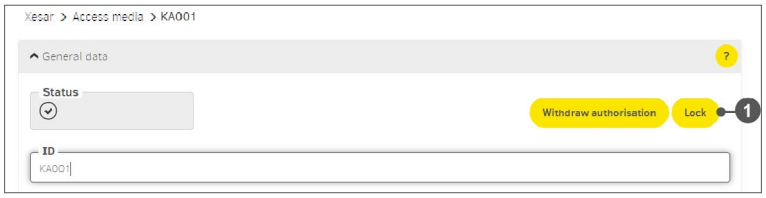
The function **Delete authorisation** ❶ is available for non-critical access media (e.g. access media of persons who should no longer have access, e.g. external companies in the building). Consequently, a blacklist entry is not created when access medium authorisations are deleted, and a warning is not shown on the dashboard.



» Click on the **Access media** menu item on the dashboard and select the affected access medium.

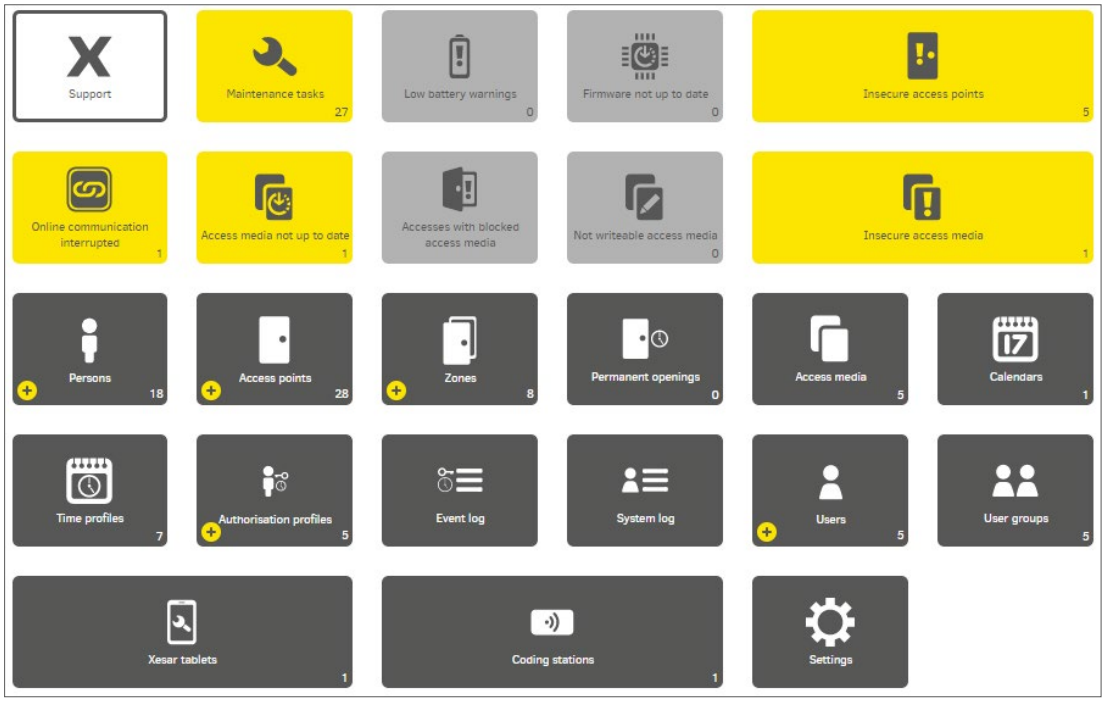
21.5.5 Blocking access medium (adding it to the blacklist)

Blocked ❶ access media are automatically added to a blacklist. The blacklist is considered to be a security risk list. Persons with blocked access media are granted access until each affected access component has been updated. This is either done via maintenance tasks using the Xesar tablet or via the XVN (Xesar virtual network).



the system is secured fastest using XVN.

The Xesar software dashboard indicates access points that have not yet been updated. A maintenance task is created for each access point and the **Insecure access point** and **Insecure access media** fields change to yellow.



21.5.6 Not writeable access media

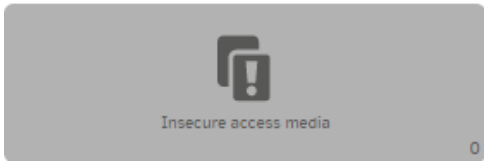
The **Not writeable access media** tile indicates that the internal memory of certain access media is full (currently: 4 kilobytes). The tile becomes yellow if access media that cannot be written to are in circulation. This is a security precaution. The right-hand side shows the number of access media that cannot be written to.

The Xesar segment on the access medium requires around 2 KB.

If the storage capacity of the access medium available to Xesar is exceeded, the colour of the field changes to yellow. A maximum of 96 areas or 32 installation locations can be allocated to an access medium. A warning is displayed if the authorisation of the access medium is extended.

Grouping together areas increases the access medium's memory capacity.

21.5.7 insecure access media



Insecure access media are created by blocking access media. In this state, the blocked access medium can still open access components (see chapter "Blocking an access medium (adding it to the blacklist)").

21.5.8 Access media not up to date

Access media must be updated after certain functions, e.g. a change in authorisation. The field becomes yellow and thus shows that access media are not up to date and must be updated.

Access media can be updated on the coding station or on the Xesar online wall reader.

21.5.9 Accesses with blocked access media

The **Accesses with blocked access media** tile indicates if and when the release of blocked identification media has been made.

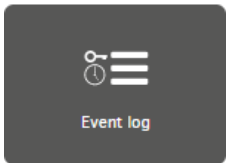
Keep the system up to date with maintenance tasks and XVN functionality.

21.6 Logs

In Xesar, two types of logs are differentiated:

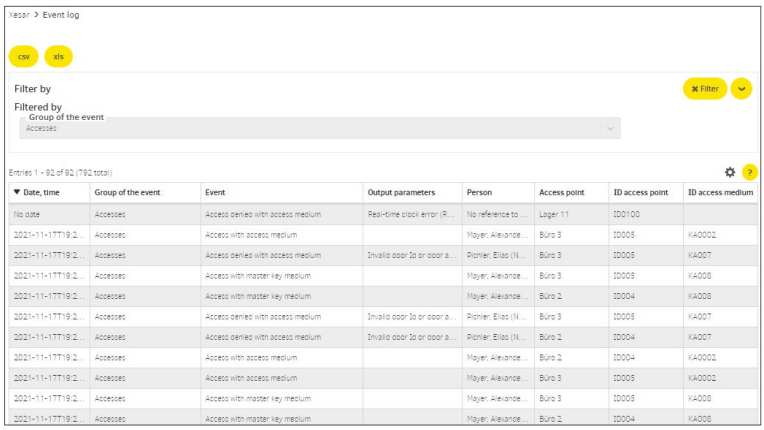
- Event log
- System log

21.6.1 Event log

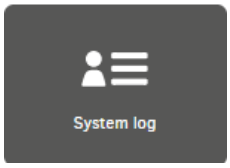


The event log shows the log entries of events that have been triggered by interaction with electromechanical locking systems (e.g. access or rejection at access components).

Event logging depends on the personal references settings in Settings as well as the corresponding event log settings on the access components, in access points, and the event log settings of individual users.



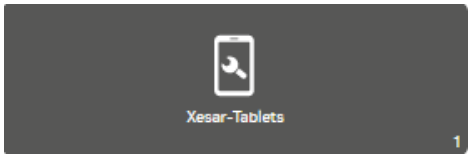
21.6.2 System log



The system log documents any actions users carry out. This means that it records events that are triggered by management tasks. In contrast to the event log, it does not record events resulting from interaction with the electromechanical access system.

» Click on the button ➔ to call up the access point and make changes.

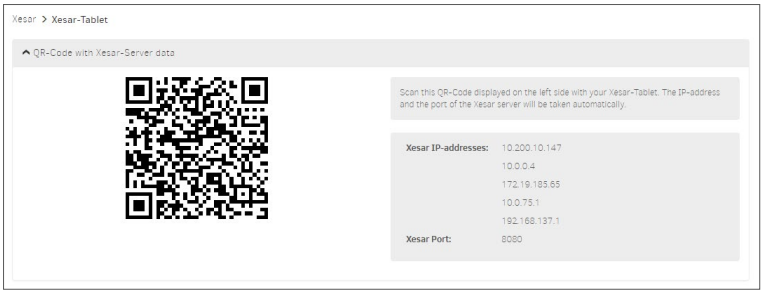
21.7 Xesar tablets (maintenance devices)



The “Xesar tablets” view shows all maintenance devices connected to the system.

QR code in list view for IP and port of systems:

» Scan this QR code with your Xesar tablet. The system’s IP address and port are automatically transferred.



» Click on the **Report loss** ❶ button to remove the Xesar tablet from the system.

For further information, see chapter “Xesar maintenance app”.

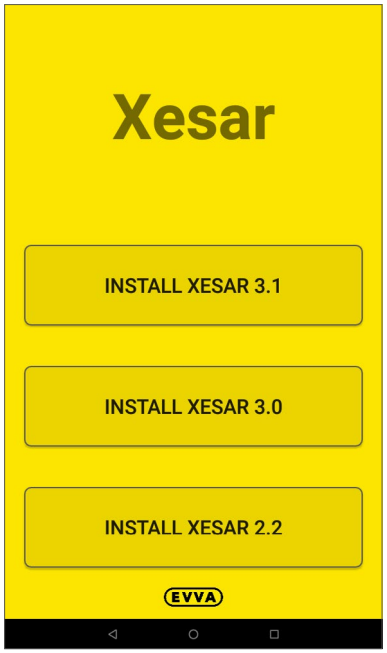
22 Xesar maintenance app

These instructions describe the operation of the Xesar maintenance app on the ARES BLE 4.2 tablet for configuring Xesar access components with a Bluetooth Low Energy communication interface as well as older access components with a USB interface.

The user interface is different if the Xesar maintenance app is operated on an older tablet than ARES BLE 4.2. (See section "Operating the Xesar maintenance app on older Xesar tablets").

22.1 Launch Xesar maintenance app

After switching on a new tablet, the start screen appears prompting selection of the desired app for Xesar 2.2 or Xesar 3.x systems.

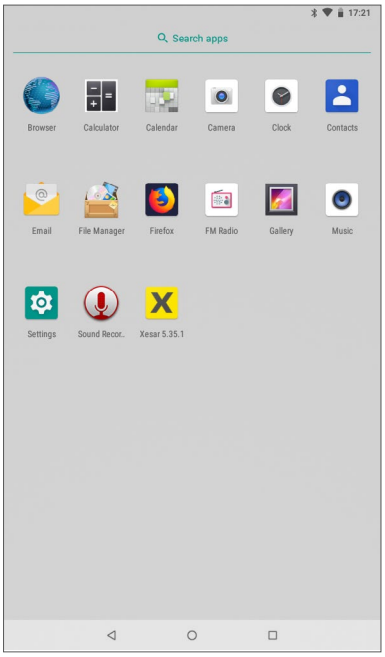


» Select the corresponding Xesar maintenance app for the Xesar version of your system.

» Xesar 3.1 and later:
Ensure that Bluetooth and the location request on your tablet as well as the Xesar maintenance app are activated and authorised. The tablet must also be on a shared WLAN network with the system PC.

» Swipe a finger on the screen from bottom to top to see all installed apps on the tablet.

» Click on the Xesar icon to start the Xesar maintenance app.



The Xesar maintenance app home page contains the following operating and display areas:

- Header:
  - Filter button
  - Settings
  - Button for logging out
- Information line
- Tab row of the two view pages
  - List of access components within range
  - List of maintenance tasks
- Display and function field
- Button for syncing with Xesar software

Yellow buttons are recommended buttons for action.
White buttons are possible buttons for action.
Grey buttons are disabled buttons.

22.2 Connecting the tablet to the Xesar software

The tablet must be connected to the Xesar software to be able to perform maintenance tasks.

» Press the **Sync with Xesar software button.** The login page opens.

The following entries are required for a successful login:

- **Name**:
  Xesar tablet (default)
  The name can be freely selected, maximum 50 characters.
- **User name** and **password**:
  access data of the user in the Xesar software.

To connect the tablet to the system, both must be on the same WLAN network.

When using several tablets in a system, each tablet must have its own name.

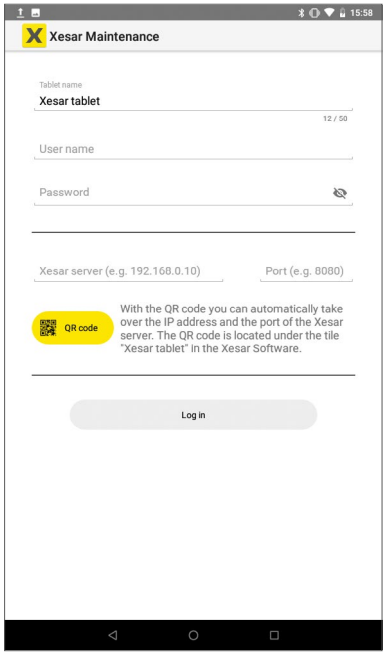
To connect the tablet to the system, the IP address and port (standard 8080) of the system must be entered in the "Xesar server" and "Port" fields.

A simpler option is to transfer the server IP address and port address using a QR code.

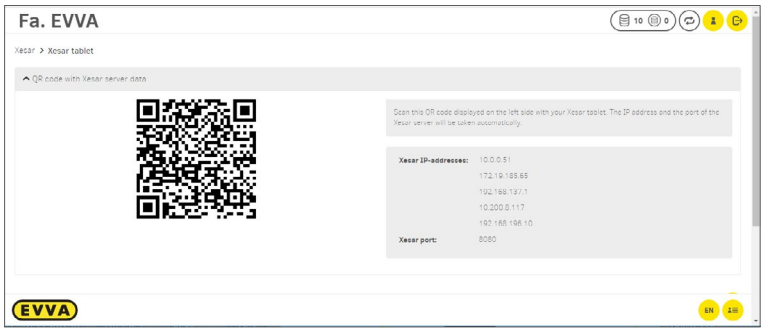
» Click the button **QR code.**
» Use the tablet camera to scan the QR code on the tablet page of the Xesar software.

The correct data is automatically transferred to the login.

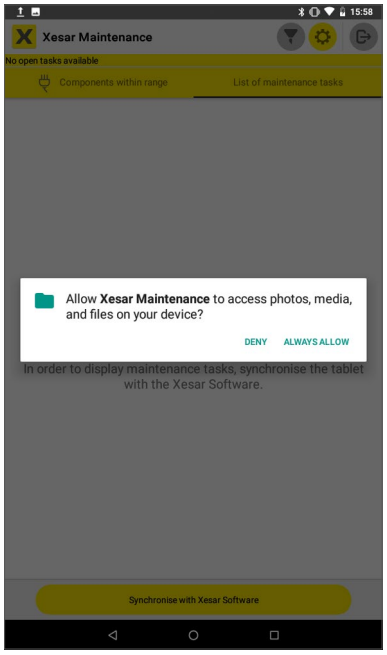
After logging out and logging in again, all entries except for the user's password are retained.



QR code with IP addresses and port addresses on the Xesar tablet dashboard page:

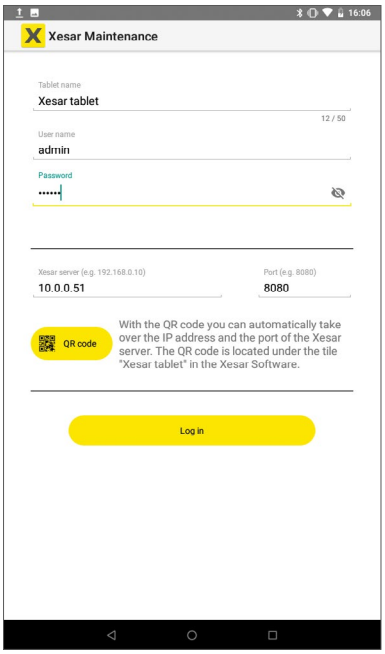


In order to use the QR code with the tablet camera, the capturing of photos and videos must be permitted on the tablet.

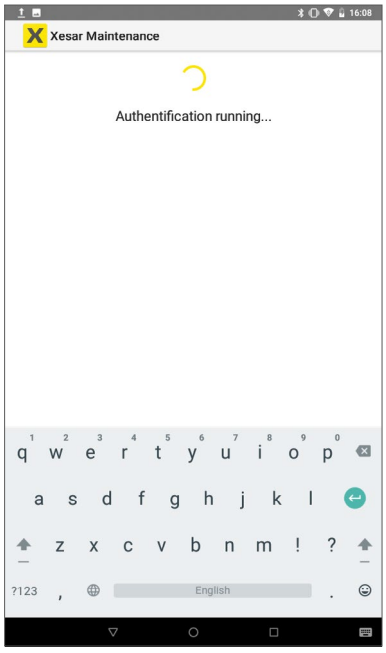


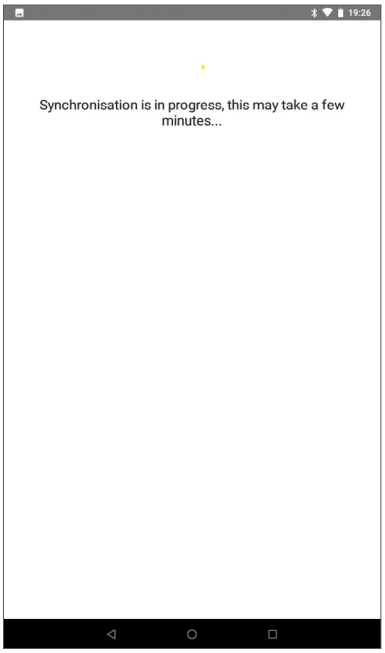
» Press the **QR code** button and point the tablet camera at the QR code in the "Xesar tablet" icon on the dashboard page. The system's IP address and port are automatically transferred to the corresponding fields.

» Click on **Log in**
When all input fields, including password, have been filled in, the "Log in" button becomes active.



After successful tablet authentication, syncing with the system will start. The maintenance tasks are transferred to the tablet.
Depending on the size and amount of data, this process may take a few minutes.





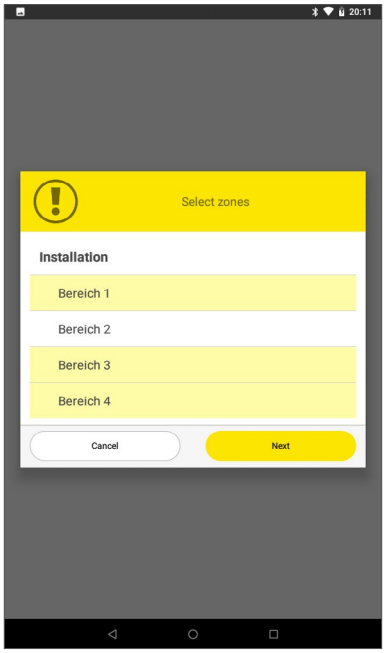
If you have assigned installation locations into different areas within the system, an option to select the areas in which to perform the respective maintenance tasks appears.

» One or more areas can be selected.

If you have not set up any areas in the system, all maintenance tasks without area selection are displayed.

The "Installation" area includes all areas and installation locations. Selecting "Installation" displays all maintenance tasks for the system.

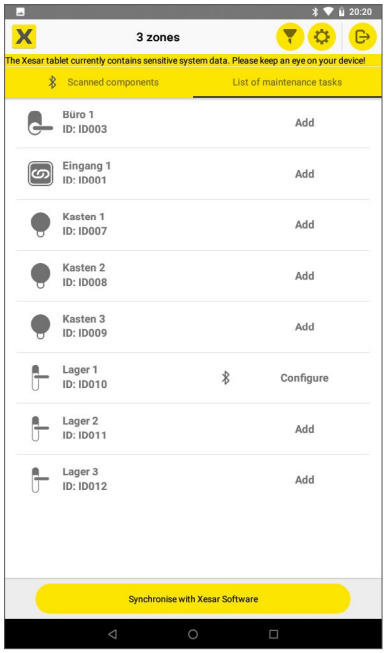
The name of the selected area or the number of selected areas are displayed in the header.



» Confirm the selection by clicking **Next**.

22.3 Maintenance tasks

After successful syncing with the Xesar software, the list of all open maintenance tasks is displayed in the display and function window



» Swipe right on the screen or click on the **Components in range** heading to switch to the “Components in range” window.

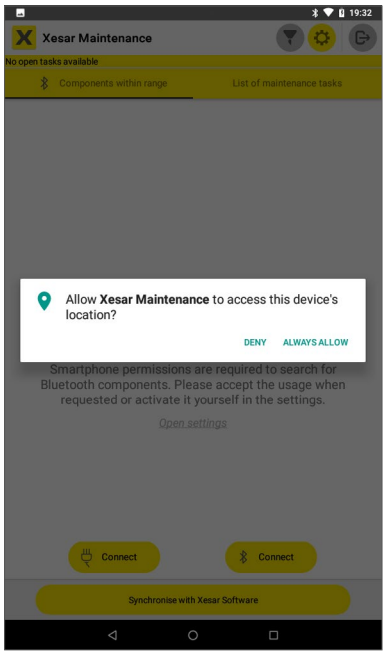
Here you can execute the open maintenance tasks after connecting to the access components.

» Click the **Connect** button to connect the tablet to all Bluetooth components Connect within range or to the access components connected by cable Connect.

22.3.1 Connecting to Bluetooth components

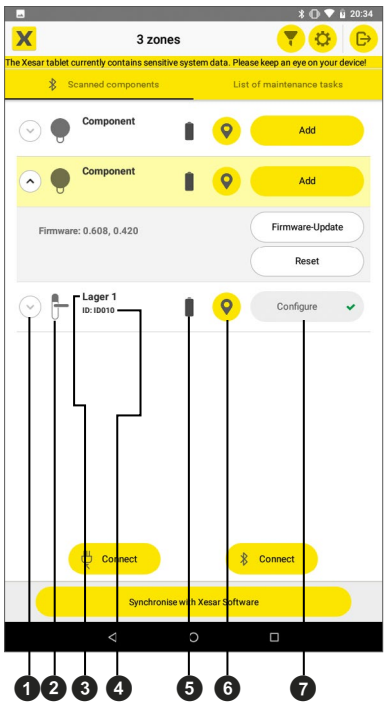
» Press the **Connect** Bluetooth (BLE) button Connect to connect the tablet to all BLE components within range. When you press the Connect BLE button for the first time, you will be prompted for the location, which you must allow.

The transmission and reception range between the tablet and BLE components depends on the structural conditions and is a few metres.



22.3.2 View connected Bluetooth components in range

Here you will find the following functions and information:



❶ Arrow button
opens and closes the additional field

❷ Component symbol
shows the component type of the installation location

❸ The name of the installation location
is displayed if the access component is installed in the system. If the access component is in construction site mode, "Component" is displayed.

❹ ID of the installation location
is displayed if the access component is installed in the system. This cannot be displayed for access components in construction mode.

❺ Battery symbol
indicates the battery status of the access component ("Battery full" or "Battery low"). If the "Battery low" signal is displayed, the batteries must be replaced immediately. (See also section "Event signalling".)

When the "Battery low" signal is displayed for the first time, a maximum of 1,000 openings are possible within a period of 4 weeks. The number of openings depends on the room temperature and may be lower as a result.

If no battery replacement is carried out and the batteries are empty, the access component can only be opened with the optional emergency power device and an access medium with general master key authorisation.

❻ Identification button

Clicking on the identification button triggers a visual and acoustic signal at the respective access component. This allows the desired access component to be uniquely identified.

❼ Maintenance task button

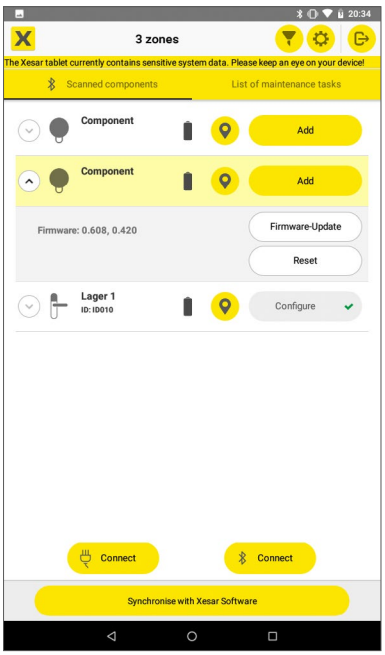
Clicking on the maintenance task button starts the corresponding maintenance task. If several BLE components with maintenance tasks are connected to the tablet, all tasks can be activated by clicking on the respective button.

The maintenance tasks are performed in the order of selection.

If a maintenance task in the queue is not to be performed, it can be removed from the preselection by clicking on the "x" icon. All other maintenance tasks will be performed.

While a maintenance task is being performed, all buttons are deactivated and turn grey.

» Use the arrow button to expand the additional field to display further information and functions. Here you will find the current firmware version of the access component and the button for updating the firmware if a newer version is available on the tablet as well as the button for resetting the access component. (See also section "Firmware update").



22.3.3 Add access component

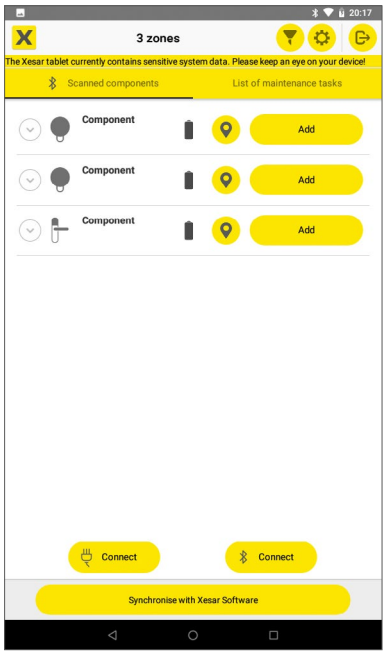
If an access component is to be added to the system, the possible installation locations for adding it are displayed.

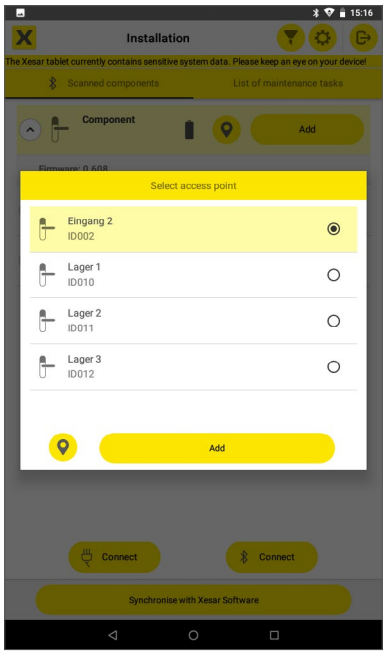
» Select the desired installation location and press **Execute.**
The access component can be controlled with the identification button for identification purposes. The corresponding access component emits an acoustic and visual signal.

The PIN code must be entered to add a new access component to the system.

The four-digit PIN code can be freely configured in the Xesar software under "Settings".

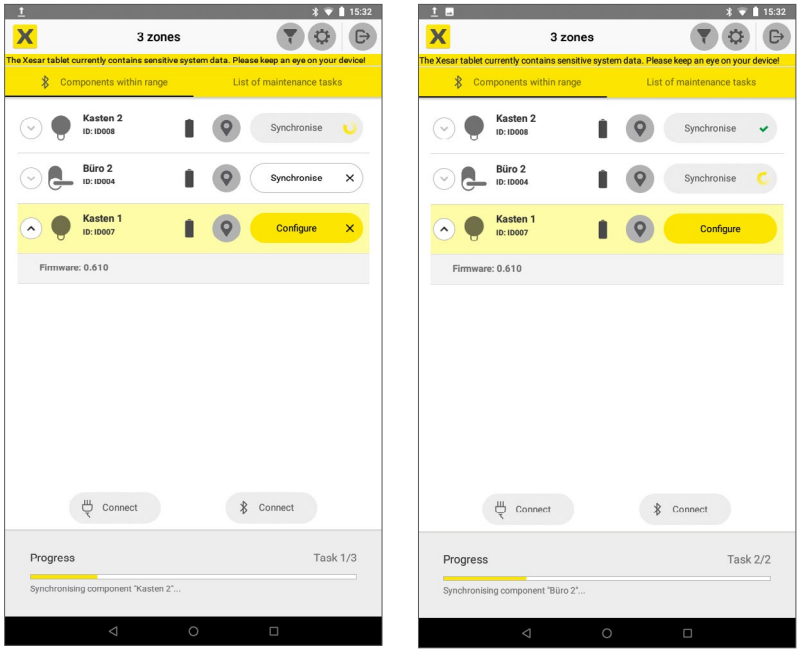
The PIN code request can also be deactivated.



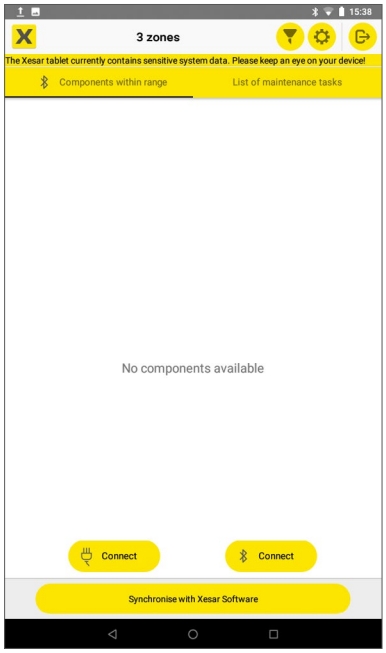


22.3.4 Multiple component configuration

To perform maintenance faster, select all maintenance tasks of the components within reach. These maintenance tasks are performed according to the order of selection. Selected maintenance tasks can be removed from the sequence by clicking again. It is not performed and remains as an “open maintenance task”.



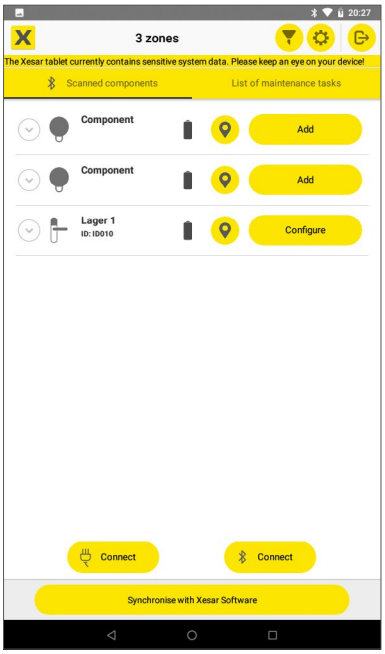
If no BLE components are within range, the following screen is displayed after pressing the BLE Connect button



22.3.5 Connecting to a wired access component

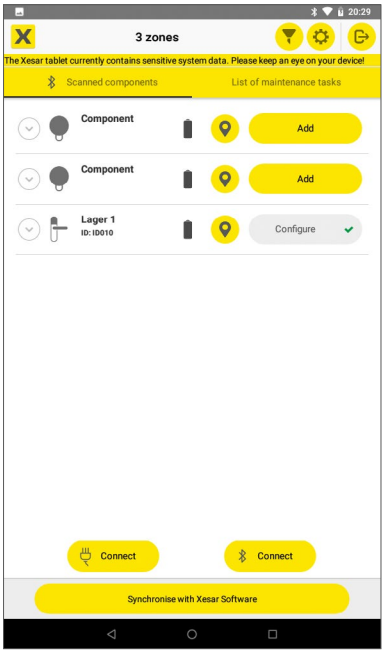
» Connect the tablet and an access component using the USB cable

» Press the **Connect** cable button. 



» Then perform the maintenance task.

The successful completion of the maintenance task is indicated by the green checkmark icon in the button.



» Sync the tablet with the Xesar software after completing all maintenance tasks. This confirms the new statuses of the access components in the Xesar software and resets the display of open maintenance tasks.

Synced access component tasks to retrieve access logs and set the time in the access components can also be carried out at any time without open maintenance tasks.
In the filter, deactivate the “Hide sync tasks” function so that access components for syncing are displayed in the list of maintenance tasks.

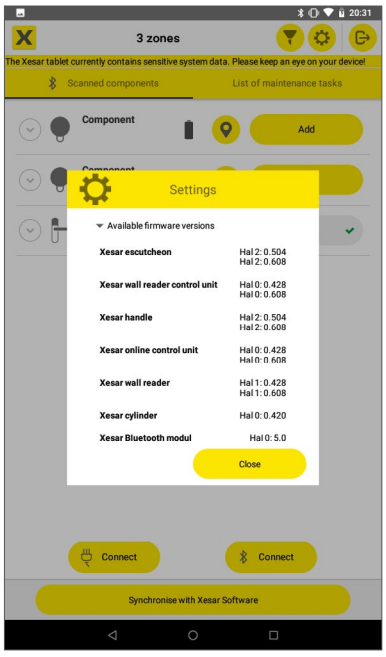
22.4 Settings

The following information can be called up and settings changed under Settings.

- **Xesar maintenance app version**
  shows the current version of the Xesar maintenance app.

- **Event log transfer**
  If the checkbox is activated, the event log is transferred from the access components to the tablet for all maintenance and syncing tasks. This can result in a longer duration of maintenance tasks. If the checkbox is deactivated, the event log is only transferred for syncing tasks. The event log contains all accesses and rejections of the access component and is transferred to the Xesar software using tablet syncing or via XVN.

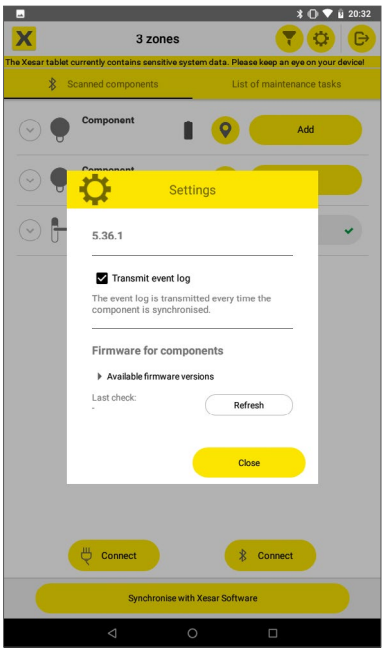
- **Access component firmware**
  shows all access component firmware versions available on the tablet.



- **Update firmware versions**
  Press **Update** to update the tablet firmware versions via the Internet from the EVVA server.

A tablet internet connection via WLAN is required to update the firmware versions.

- **Last check**
  Date of last successful check of firmware versions



22.4.1 Firmware update

Firmware updates ensure safe and smooth operation of the system. They enable functional improvements and new access component features.

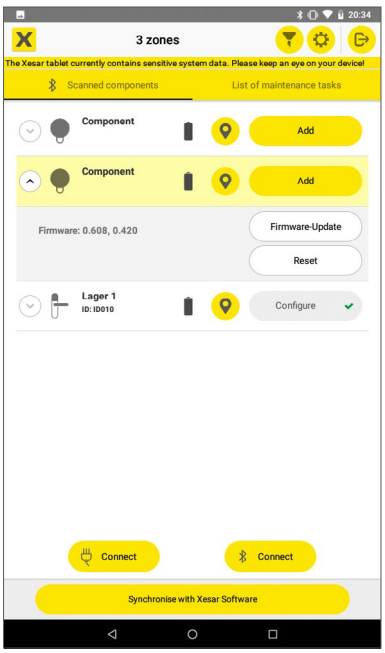
Access components with outdated firmware are displayed on the dashboard.

The firmware versions contained in the Xesar software are loaded onto the tablet by syncing the tablet with the Xesar software. If an access component has an older firmware version, this access component can be updated with a firmware update.

A maintenance task is created for the firmware update of an access component and displayed in the list of maintenance tasks.

» Connect the access component to the tablet (via cable or wirelessly via BLE).

» Perform the maintenance task by clicking on the maintenance task button.



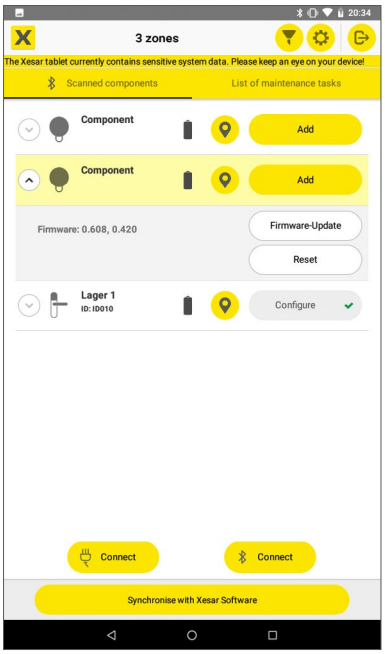
22.4.2 Firmware update in construction mode

If an access component is in construction mode, a firmware update can be performed even if the tablet is not connected to a system.

Keep the firmware of all access components up to date and always carry out firmware updates.

If a newer firmware version is available than the one installed in the Xesar software, the new firmware version can be downloaded to the tablet by updating it under “Settings” on the tablet. To do this, the tablet must be connected to the EVVA server via the Internet WLAN. This current firmware can be loaded onto the respective access components as required as described above. No maintenance tasks are created for this.

» In the “Components within range” view, expand the detailed view of the respective access component and perform the firmware update.



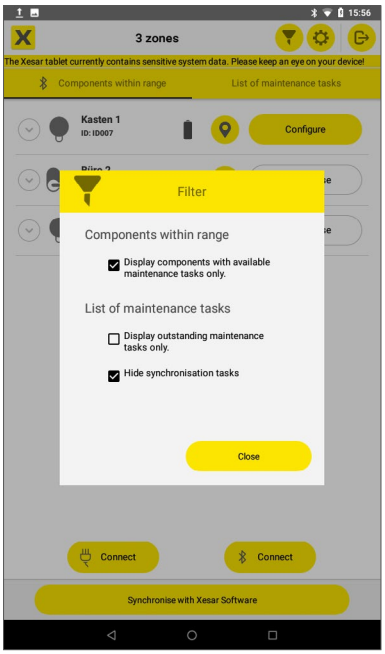
22.5 Filter

Under the filter options, settings can be selected for the “Components in range” and “List of maintenance tasks” pages.

- **Display only components with existing maintenance tasks**
  If the checkbox is activated and a scan is performed, then only the BLE components in range for the relevant system and access components in construction mode for which a maintenance task is available are displayed. Access components of other systems that are also within range are not displayed.
  If all existing access components are to be displayed within range, the checkbox must be deactivated.

- **Enable the list of Maintenance Tasks**
  “Show Open Maintenance Tasks Only” to show only the maintenance tasks that are still open. Tasks that have already been completed are hidden.

- **Hide sync tasks**
  If this box is checked, only access components with maintenance tasks are displayed in the maintenance task list and access components with possible sync tasks are hidden.



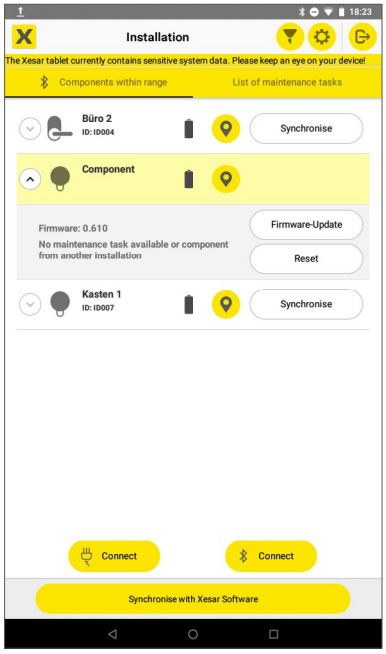
22.6 Resetting an access component to construction mode

If an access component has been removed from the system in the Xesar software, it is reset to construction mode after the corresponding maintenance task has been performed. In this state, it can be added at another installation location or in another system.

A faulty access component is removed from the system in the Xesar software via “Remove faulty component”.

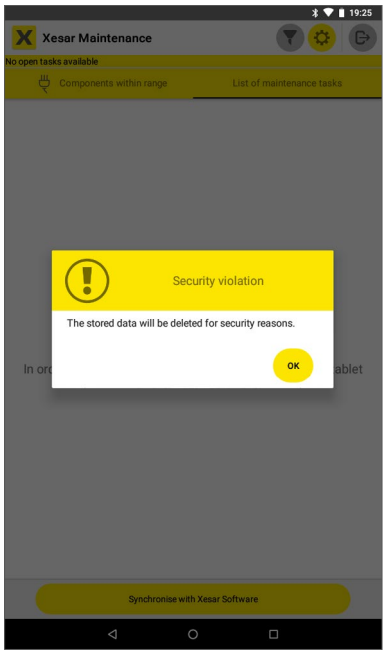
If an access component is accidentally removed as defective, it can be set to construction mode by resetting it on the tablet and then re-adding to the system. If the component is reset via BLE, the “Show configuration tasks only” filter must be deactivated so that the component can be found via BLE scan.

If an access component with deactivated BLE transmission function is reset to construction mode, the BLE function is activated.



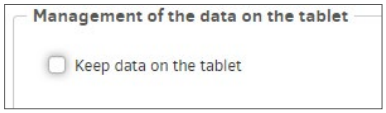
22.7 Other displays

If the time or location data of the tablet is changed in the operating system, the data stored on the tablet is deleted for security reasons and the following message is displayed:



22.8 Managing tablet data

If data should remain saved for later maintenance tasks after switching off the tablet, select “Keep data on tablet” on the dashboard under “Settings > Managing tablet data”.

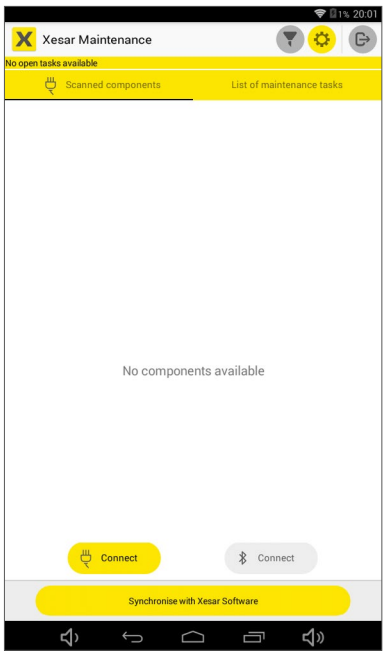


If this box is checked, security-related data remains on the tablet even after the tablet has been switched off.
Make sure that the tablet is only operated by authorised persons.

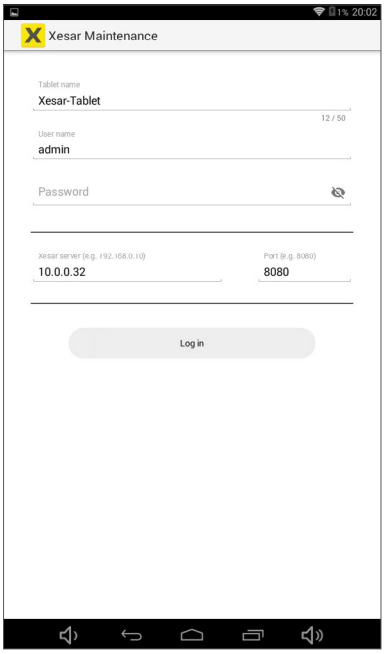
22.9 Operation of the Xesar maintenance app on older tablets

The Xesar maintenance app can also be operated on an older tablet, as ARES BLE 4.2. However, due to the lack of BLE and camera functions, the following actions cannot be performed:

- Wireless configuration of G2.1 BLE components
  (connect button is deactivated; wired connection is possible)



- QR code scanning is not possible.
  (The IP address and port number for tablet syncing must be entered manually.)



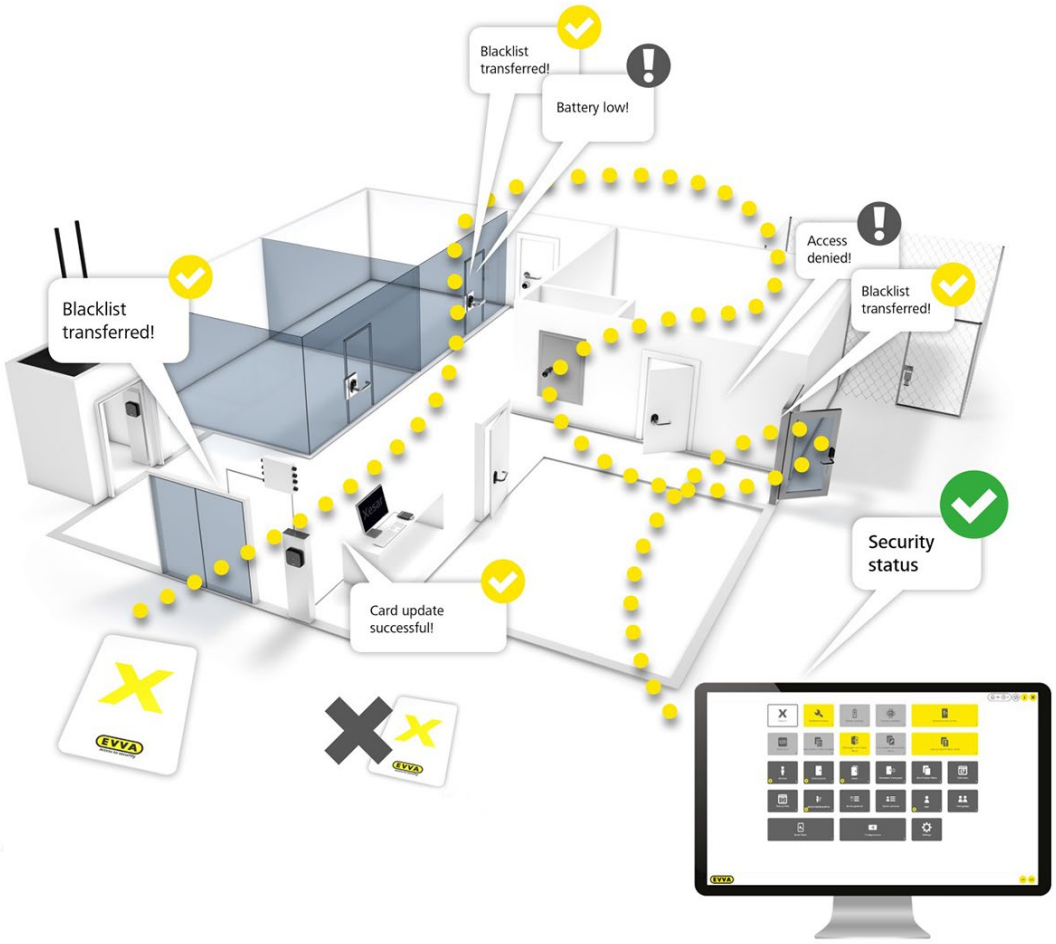
23 Xesar tablet error messages

Incorrect handling of a Xesar tablet may cause a host of different error messages. Below is an overview of all error codes as well as some information on the cause and troubleshooting.

Error code	Error message	Causes and troubleshooting
XTDE01	Incorrect component type	A different access component was detected in the Xesar software for this installation location. » Check the correct installation location and the corresponding Xesar component type.
XTDE02	USB not connected	The USB cable is not correctly connected to the tablet or access component or the USB cable is defective. » Check the plug connections and the condition of the cable.
XTDE03	No response	An error has occurred on the tablet or access component. » Restart the tablet.
XTDE04	Incorrect door	Access component is located on the wrong door. An old database may have been restored. » Check installation location or validity of the database.
XTDE05	No battery in component	» Insert the specified batteries into the access component in the correct polarity or » replace any empty batteries.
XTDE09	Sub-component unresponsive	The cylinder knob has not been installed correctly or the wall reader has not been wired correctly. » Check the access component for correct assembly and connection.
XTDE10	Version not supported	The access component does not have the correct firmware version. » Perform a firmware update in construction mode with the tablet.

Error code	Error message	Causes and troubleshooting
XTDE11	USB communication error	The USB cable is not correctly connected to the tablet or access component or is defective. » Check the plug connections and the condition of the USB cable. » Check whether the access component is faulty.
XTDE12	Unknown error	Unknown cause. » Try to log out the tablet and sync it again with the Xesar software.
XTDE13	Operation failed temporarily	» Try to log out the tablet and sync it again with the Xesar software.
XTDE14	Operation failed	» Try to log out the tablet and sync it again with the Xesar software.
XTDE15	Xesar tablet not synced	Sync the tablet with the software.»
XTDE16	Failed to show battery status	» Check the batteries in the access components and replace them if necessary.
XTDE17	----	The reset of a Xesar component that has been forcibly removed from the database has failed. » The access component must be sent to EVVA for repair.

24 Xesar virtual network (XVN)



Access media are provided with update information (blacklist) from a central location (coding station or Xesar online wall reader). The information is transferred from door to door on the way through the facility. In this process, access media update door states and collect door information (battery status, access events, deletions or openings by blocked media). The information is subsequently passed on to coding stations, evaluated and the security status in the software is updated.

Up to 150 Xesar online wall readers can be integrated into one system.

24.1 Transferring access events via access media

The most recent Xesar access component events (e.g. access granted, access denied, battery low) are transferred to the access medium with every second identification process, e.g. when an access component is unlocked using an access medium.

If the access medium is held to the coding station or the Xesar online wall reader, the events are transferred to the Xesar software and the access medium is cleared.

A login of the Xesar software is not necessary for this process, it is sufficient when the program is running.

24.2 Transferring blacklist entries using access media

A blacklist entry contains information regarding access media that are blocked in the Xesar software. These blacklist entries are written to all access media by the coding station or online wall reader. In this way the information is transferred to all operated access components.

Up to 10 blacklist entries are possible on one access medium. As soon as the access media are presented to the coding station or the Xesar online wall reader, the Xesar software recognises to which Xesar access components the blacklist has already been transmitted by the respective access medium and visualises the corresponding status on the Xesar software dashboard.

Transfer the blacklist via Xesar tablet if more than 10 identification media are lost or stolen simultaneously.

An access medium blocked in the Xesar software can be invalidated or deleted if:

- the expiry date is exceeded
- the validity period has expired
- the access medium has been presented to the coding station or the Xesar online wall reader
- the access medium attempts to open an access component for which the blacklist is current.

24.3 Transferring the information “Accesses with blocked access media”

As long as a blocked access medium is still valid in the Xesar software, it can also open the respective access components. This type of information is critical to security and the data is collected by other access media within the system before it is transferred to the Xesar software via the coding station or Xesar online wall reader.

The dashboard indicates this. The colour of the **Accesses with blocked access media** tile becomes yellow if openings with already blocked access media have taken place.

24.4 Transferring the information “Access medium deleted from access component”

The access medium is deleted from the access component upon attempting to unlock an access component (with an up-to-date blacklist) using an access medium that has been blocked in the Xesar software.

Subsequently, this access medium cannot open an access component unless the blacklist is up-to-date. This access medium has thus lost its validity.

The information from a blocked or deleted access medium is returned to the Xesar software by other access media via the virtual network. This requires the access media to be held against a coding station or a Xesar online wall reader.

This automatically informs Xesar software users that the system is once again secure even if the blacklist has potentially not yet been transferred to all access components.

Follow the instructions for possible maintenance tasks in the dashboard and keep your access components up to date.

24.5 Transferring the battery status using access media

Battery information is also transported to the Xesar software via the virtual network using the access media in circulation. The system administrator thus knows in good time when to replace which batteries.

System administrators have the option to indirectly influence update cycles using the access media's validity periods. The validity period is automatically extended by the set value each time an access medium is presented to the coding station or the Xesar online wall reader.

If, for example, the validity period is set to 3 days, every person with an access medium must carry out an update at the coding station or the Xesar online wall reader within this time period in order to extend the validity. Thus the system administrator receives the corresponding information (e.g. events or blacklist transfers) via the circulating access media at the latest within 3 days. For instance, if the validity is set to 30 days, it will take longer for the information to be returned to the Xesar software.

When using the virtual network, keep the validity period as short as possible, preferably under 15 days.

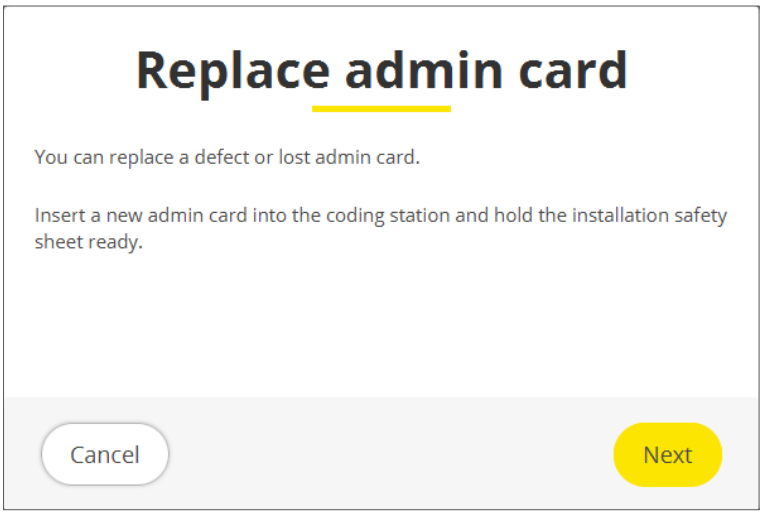
25 Replacing Admin Card

25.1 Replacing Admin Card for Xesar installations on PC

Also see chapter "Installation Manager start page > System configuration".

If the system's Admin Card is defective or lost, it can be replaced with a new Admin Card.

» To do this, click **Replace Admin Card** on the configuration page and follow the instructions.



25.2 Replacing Admin Card for Xesar installations on server

If the Admin Card is defective or is lost, then it can be replaced as follows:

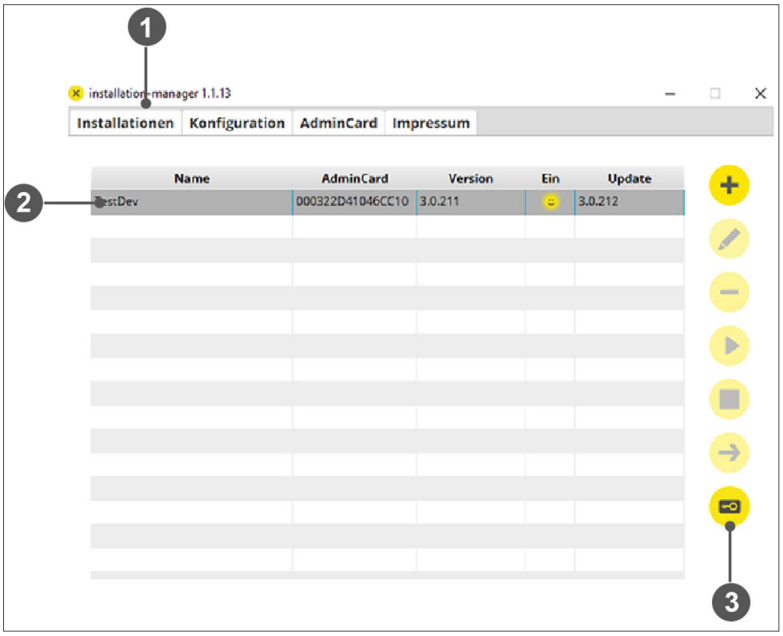
» Insert a new Admin Card in the coding station.

» Open the **Admin Card** tab in the Installation Manager and load the new Admin Card.

» Save the setting and then change to the tab **Installations** ❶.

» Select the desired system ❷ and

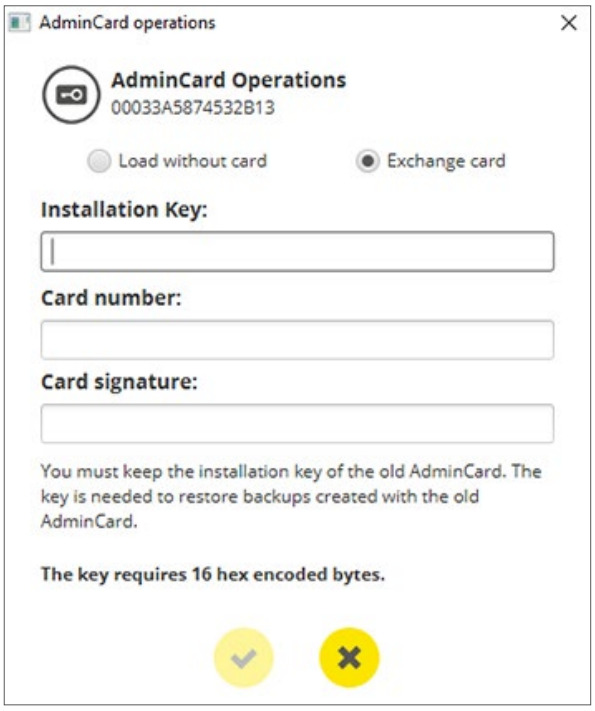
» Click on the **key** ❸ symbol.

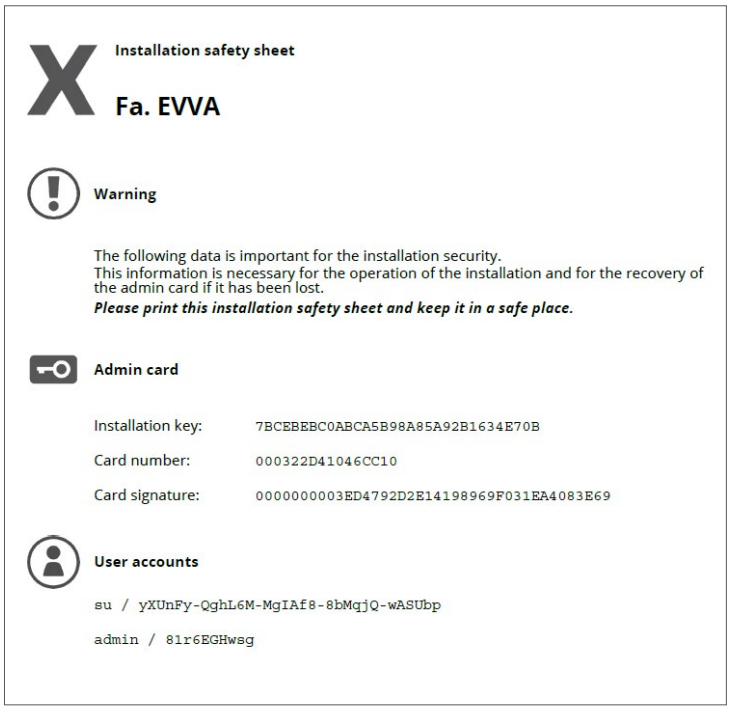


» In the "Admin Card operations" window, select the **Replace card** function.

» Enter the installation key, the card number and the card signature.

This data can be found on the installation safety sheet that you printed out during the first installation.





A new installation safety sheet is generated after confirmation.

» Print out this installation safety sheet and keep it safe.

After replacing the Admin Card, be sure to create a manual backup in the Xesar Installation Manager, so that it will match the new Admin Card if a restore is necessary.

25.3 Undo the process of adding a component

If the wrong component was added at the access point, you can remove the component again.

» Click on the button **Undo adding component** ❶.

Furthermore, you don't have to recreate the access point, you can simply select a new access component.

This procedure only functions before adding the access component and, if necessary, after resetting to construction site mode.

25.4 Removing components (resetting to construction mode)

Select **Remove component** if you would like to once again remove an access component and continue to use it.

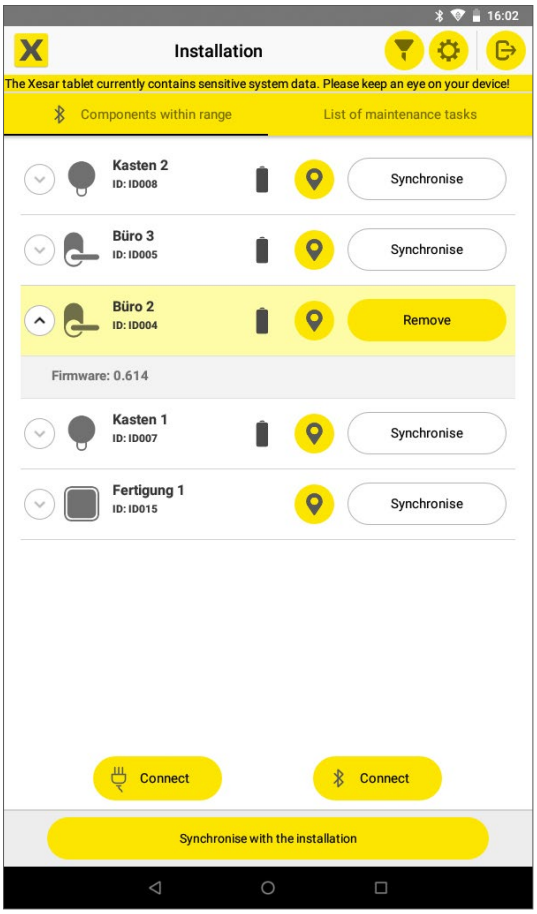
If you would like to once again install the component in a system, do NOT click **Remove faulty component**.

If you have removed the access component in the Xesar software, a maintenance task is automatically created. The access component must be removed with the Xesar tablet.

» Connect the access component to the Xesar tablet and

» select the access component on the Xesar tablet.

» Execute the **Remove** maintenance task.



25.5 Force component removal (component faulty)

If an access component is faulty, proceed as follows:

- Select the appropriate access points in the access points menu.
- Select the access components to be removed in the list and
- Click on **Remove faulty component**.

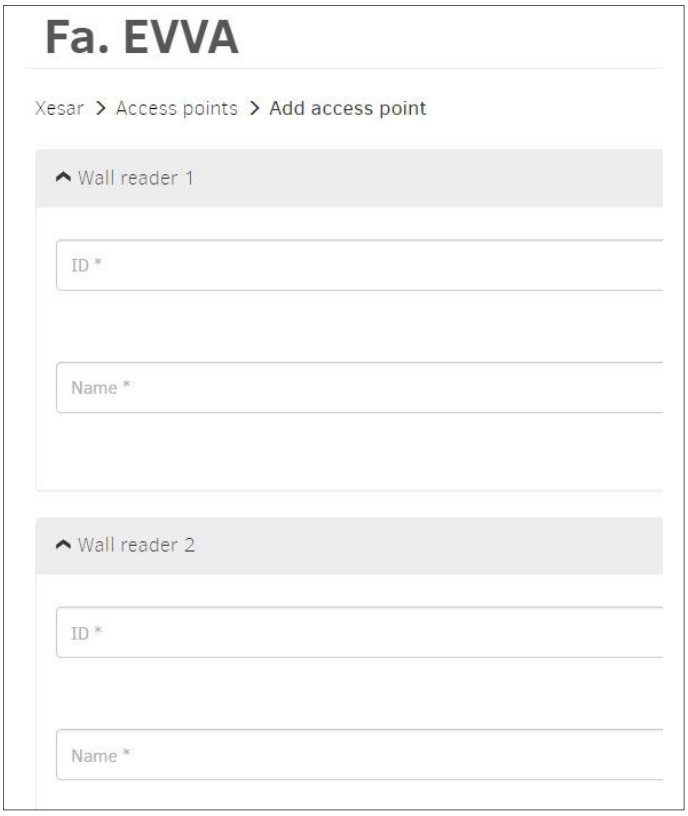
26 Offline control unit with 2 wall reader

26.1 Add wall reader

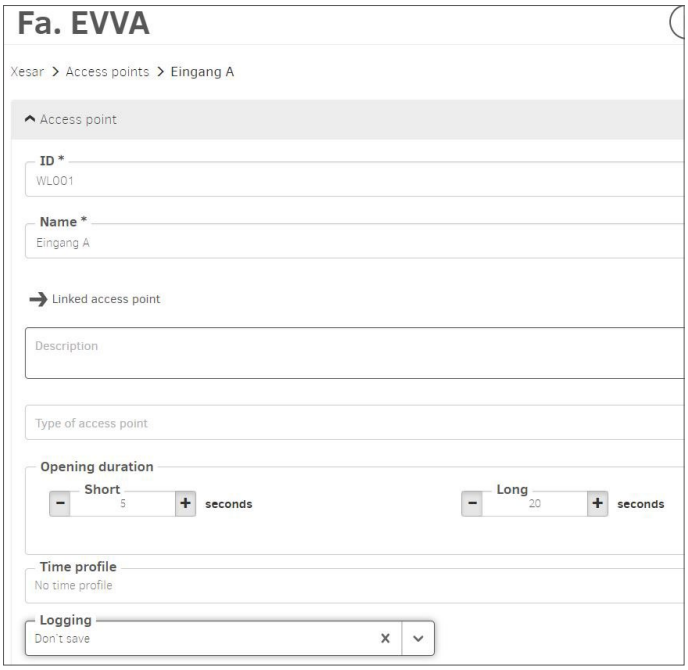
You want to equip 2 installation locations (doors) with a wall reader and a common control unit.

» Under “Add installation location”, select the component “Xesar control unit with 2 wall readers” to add 2 wall readers with an offline control unit.

» Enter the IDs and names in the fields of the two desired installation locations.



» Configure the two installation locations by clicking → Linked access point to switch between the two installation locations.



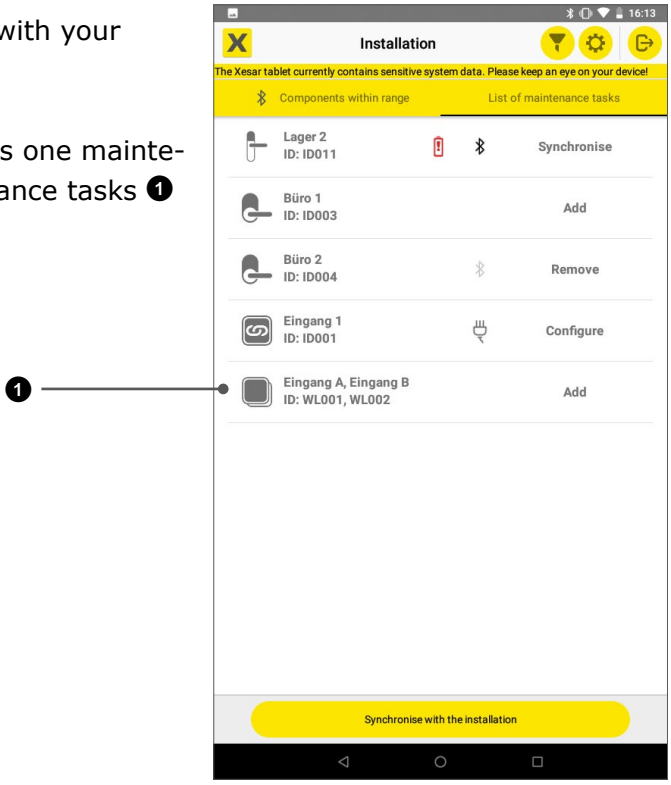
After confirming the entries, both wall reader installation locations are created in the system and maintenance tasks for adding them are created.

The list of installation locations describes the two linked wall readers with the status “Prepared for adding”.

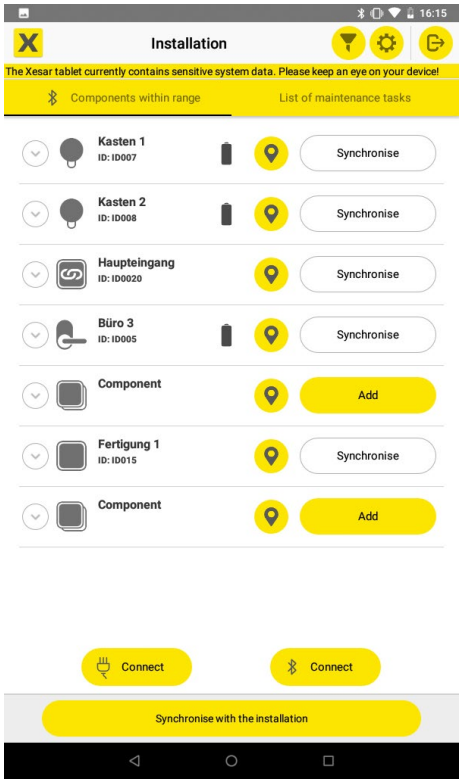
Not connectable	WL001	Eingang A	Eingang A	Automatik Tür		Prepared for adding
Not connectable	WL002	Eingang B	Eingang B	Automatik Tür		Prepared for adding

» Synchronise maintenance tasks with your Xesar tablet.

The two wall readers are listed as one maintenance task in the list of maintenance tasks ❶ on the Xesar tablet.

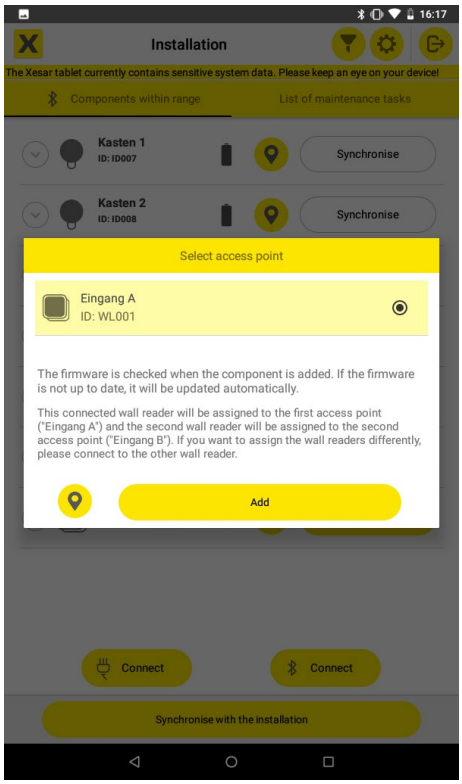


» Connect your Xesar tablet to the wall readers and perform one of the two maintenance tasks.



» Before adding the selected wall reader, check the correct assignment to the installation location using the identification function.

The following message appears on the tablet:



» If the assignment is not correct, select the other wall reader.

The second wall reader is automatically added to the second installation location.

When adding, the current status of the firmware is checked and updated if necessary.

26.2 CU – carry out maintenance tasks for 2 wall readers

You must perform the maintenance tasks for the respective wall reader directly on the corresponding wall reader.

» Connect the Xesar tablet to the respective wall reader and

» perform the maintenance tasks.

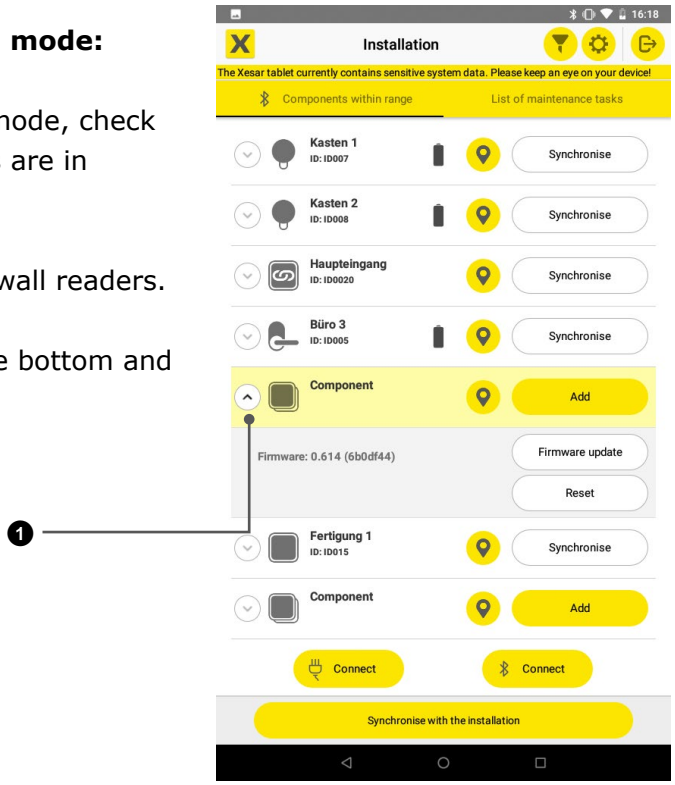
26.3 CU – firmware update of 2 wall readers

All sub-components (wall reader and control unit) must have the same firmware version in order for the wall readers to function correctly.

Perform a firmware update for the wall readers and the control unit as follows:

Firmware update in construction mode:

- With a medium in construction mode, check that the wall reader components are in construction mode.
- Connect the Xesar tablet to the wall readers.
- Click on the arrow ❶ to open the bottom and
- perform the firmware update.



If components with different firmware versions are combined in the course of a wall reader or control unit replacement, the subcomponents must be switched to construction mode and then updated to the current firmware version.

26.4 Remove wall reader components from the system

» Select **Remove component** at the installation location in the software and confirm the selection.

» Synchronise the Xesar tablet with the software.

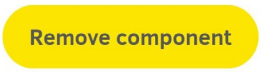
» Connect the Xesar tablet to the wall readers and perform the maintenance task **Remove** on a wall reader.
The second wall reader is also automatically removed.

After removal, the components are in construction mode.

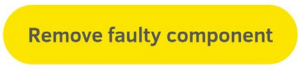
If required, you can now perform a firmware update and reinstall the components in another or the same Xesar system.

If one or more components are defective:

» Select **Remove component at the installation location in the software**



» Then select **Remove defective component**.



The component removed as defective must be replaced.

If you have mistakenly removed a functioning component from the system using **Remove defective component**, you must synchronise the Xesar tablet with the software. Then connect the Xesar tablet to the component that was removed by mistake and reset it to construction mode by clicking **Reset**. The reset component can be reintroduced into the installation.

27 Xesar online wall reader

The Xesar online wall reader reads information from the access media collected with the XVN (Xesar Virtual Network) and provides it to the Xesar software for further processing. These data include, for example, access events, rejections or the battery status of access components. At the same time, the current blacklist is written to the access media and the validity period of the access media is extended or the access media-15 is executed. The Xesar online wall reader also serves as a control unit for electrically driven access components, such as motorised locks and cylinders as well as automatic door drives. The locking status of the door can be monitored and displayed if a door contact is connected.

Xesar online wall readers offer the following functions:

- Update access media (authorisation changes, validity period, blacklist).
- Access events Real-time log entries.
- Configuration changes to the Xesar online wall reader in real time.
- Function for identifying a Xesar online wall reader: the Xesar online wall reader being searched for emits a repeated visual and acoustic signal until the function is deactivated.
- Start and stop office mode: Start and end of manual office mode is logged.
- Set time: manual time synchronisation with Xesar online wall reader (is logged) e.g. after power failure = offline.
- Perform remote opening: A logged remote opening is performed at the push of a button.
- Normal release: Default release duration is logged.
- Extended release: Extended release duration is logged, e.g. for persons with restricted mobility.
- Door exit button: for opening automatic doors or separation systems.
  Each operation of the door exit button is recorded in the event log.
- Door status monitoring Query the status of the door contact (open or closed).
  If the door contact is connected in series with a bolt contact, the **closed** and **locked** door status can be monitored.

The various functions are logged in the event and system logs.

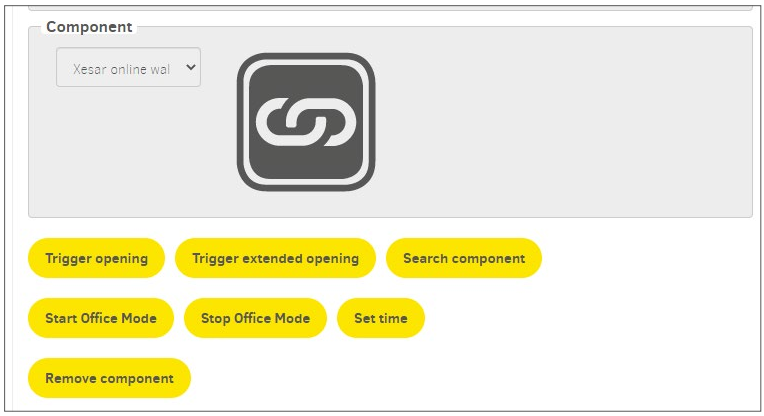
27.1 Add Xesar online wall reader

» Add a new installation location to your system and select the Xesar online wall reader in the "Component" field.
» Click **Continue**.

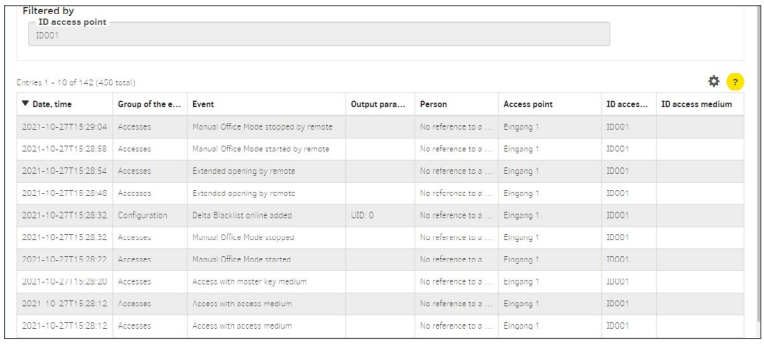
» Enter the relevant data and
» select the desired settings.

- Allow access:
  - When activated, the Xesar online wall reader functions as a media updater and as an access component.
  - When deactivated, the Xesar online wall reader functions as a media updater.
- Allow upgrade of an access media:
  - If activated, an upgrade of access media is possible. This may be necessary due to changes to the media data format.

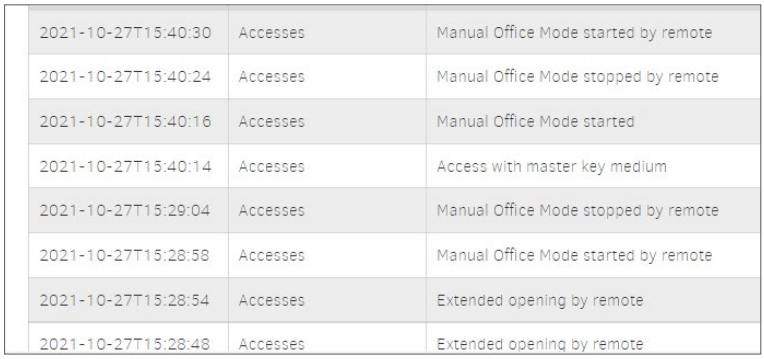
For safety reasons, this function is deactivated at the factory and should only be activated if necessary.



Event log door status monitoring:



The various functions are logged in the event and system logs.



28 Commissioning the Xesar-Online Wall Reader Network Adapter EXPERT EX9132CST

Check that you have the appropriate model in use as per the setup guide before configuring the network adapter.

Additional network adapter commissioning instructions:

› **https://www.evva.com/uk-en/service/downloads/**

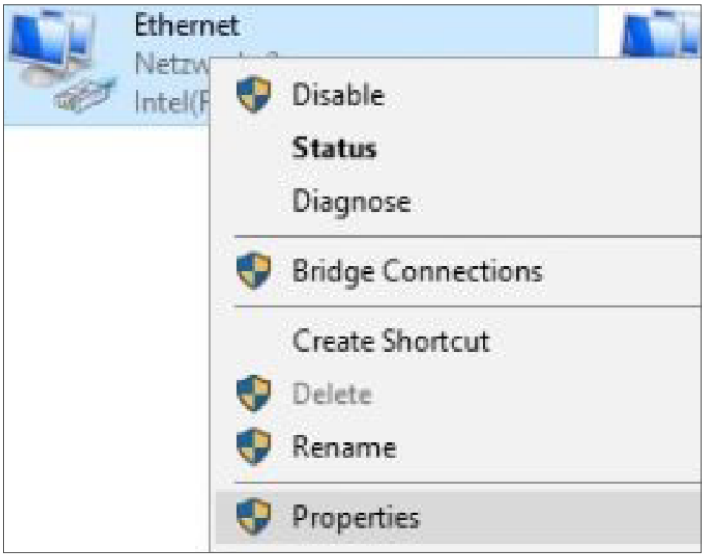
Please contact your EVVA technical office if you have any questions or would like to obtain more information.

28.1 PC configuration

Any computer is suitable for configuring the Xesar network adapter. This can also be the PC on which the Xesar software is operated.

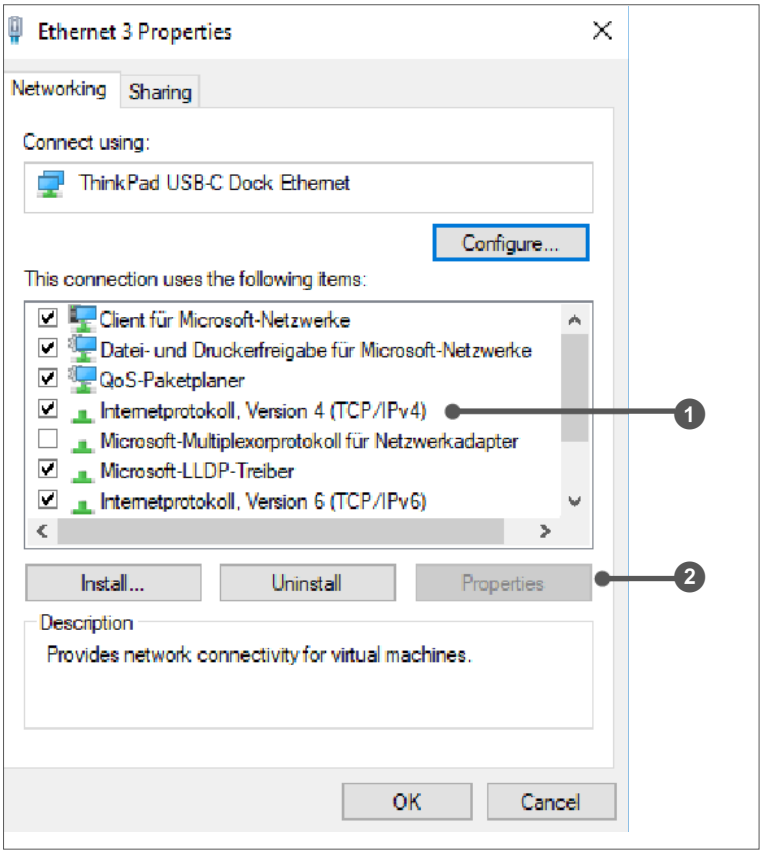
Please configure the settings of your PC network adapter before starting to commission the Xesar network adapter. For this purpose, e.g. in Windows 7 or Windows 10, go to Network and Sharing Center > Change adapter settings.

» Open the Settings window (right-click the LAN connection).



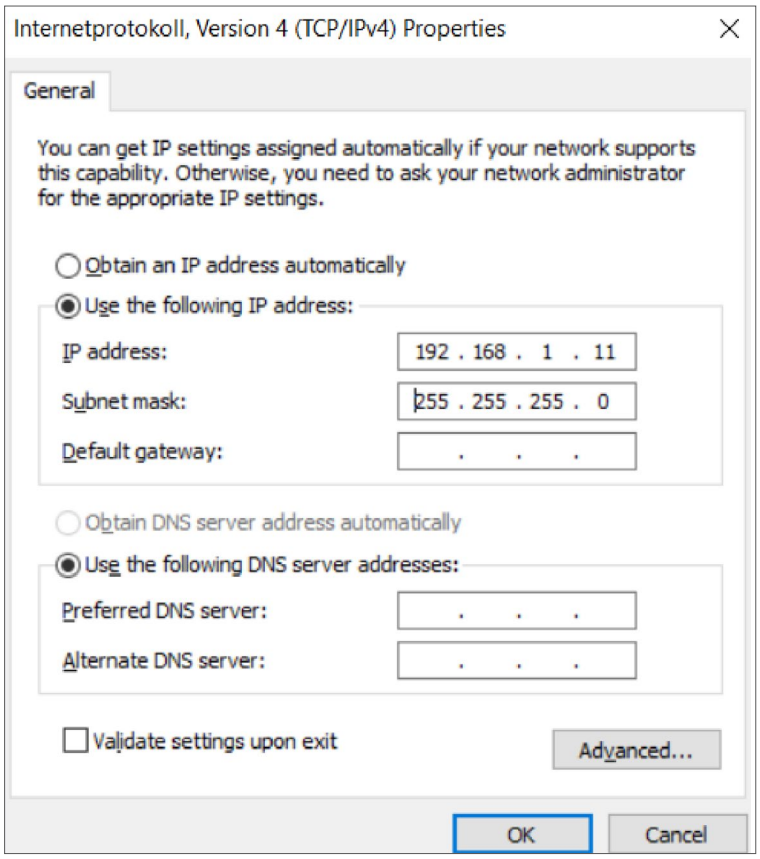
Please note that additional active network connections (WiFi, etc.) may impair communication with the Xesar network adapter. Switch them off if necessary.

» In the window, select Internet protocol version 4 (TCP/IPv4) ❶ and click Properties ❷.



» The IP address and the subnet mask of the PC 1 must be configured in order to configure the Ethernet Adapter. Use the following addresses for this purpose:

IP-Adresse: 192.168.1.xxx (1-254)
Subnetzmaske: 255.255.255.0
DNS-Server: -



To avoid an IP address conflict, be careful **NOT** to use the default IP address of the Xesar network adapter (**192.168.1.100**).
(If there is an IP address conflict, a connection can not be established.)

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

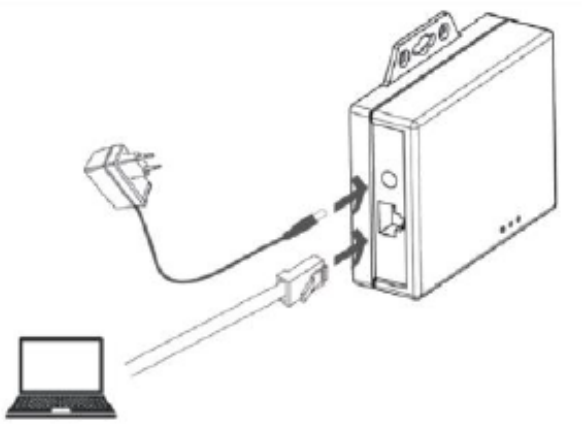
28.2 Commissioning a Xesar network adapter

» 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.



» Open the Internet browser on your computer.

» Enter the standard address of the Xesar network adapter in the browser's address bar – this can be found on the bottom of the device, it is set to **192.168.1.100** by default.

If you cannot open the configuration page, check the firewall settings of your PC, the IP settings, and also the correct wiring of the Xesar network adapter.

You will be directed to the system page of the Xesar network adapter.

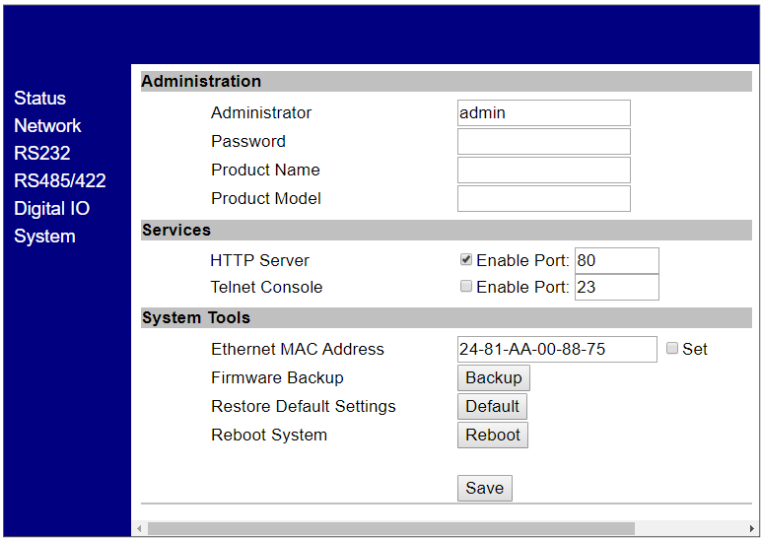
28.3 Status page

» On the status page, enter a password for security. This is optional and not absolutely necessary. The default administrator name used to login is "admin". No password has been assigned.

» The Device name can be individually configured and it does not influence the device function.

» The Login password restricts access to the device configuration page.

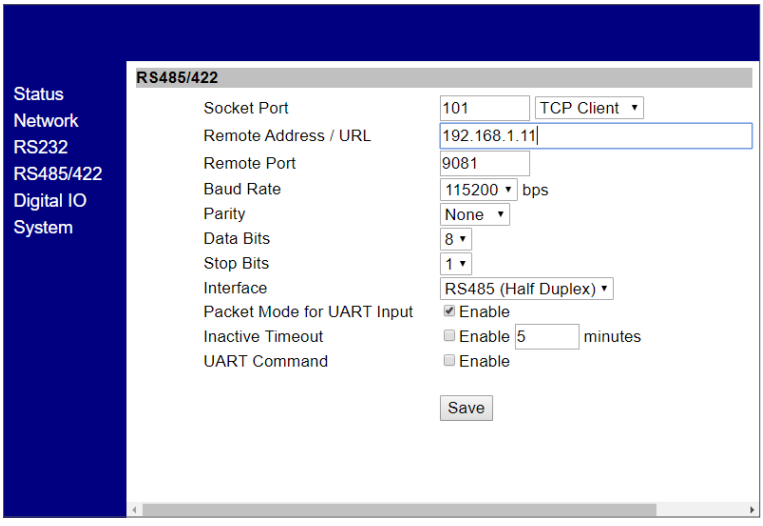
A default password has not been configured.



28.4 RS485/422

» In the “Remote Address /URL” field, enter the IP address of the PC or server on which the Xesar software is installed.

It is responsible for the communication between the Xesar network adapter and the Xesar software. It is important that the remote port (9081 by default) is the same as that specified in the Xesar Installation Manager (OCH Port).

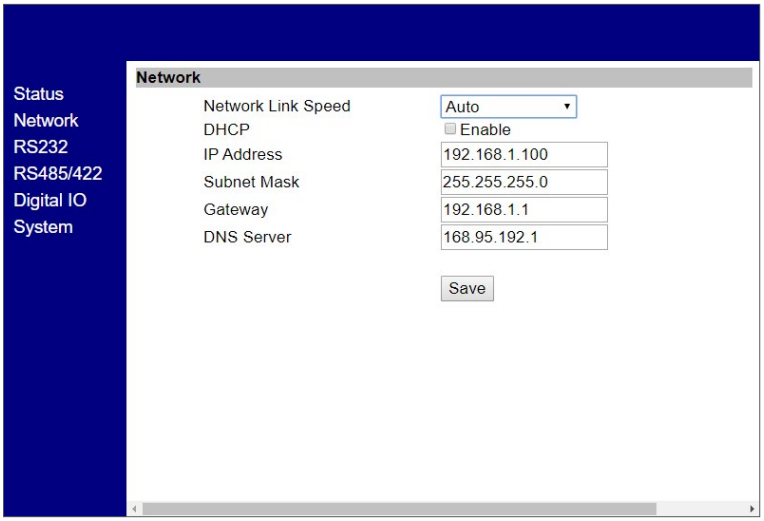


28.5 Network

» On the Network page, the fields are to be filled in as shown below.

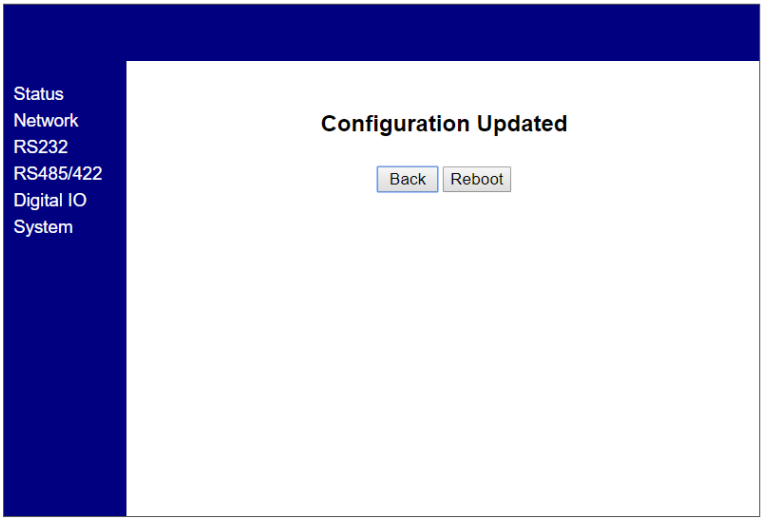
The IP address defines the IP address of the Xesar network adapter.

Please note: if the address is changed and **Save** is clicked (or by confirming with the ENTER key) then the network adapter can exclusively be opened and configured using this address.



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

» To transfer the data to the Xesar Ethernet Adapter, press “Reboot”.



» After rebooting the network adapter, disconnect the Xesar network adapter from the configuration PC.

» Then connect the Xesar network adapter to the Xeasar LAN network.

Typically 150 different IP addresses can be defined for the Xesar network which means that you must define as many as 150 different IP addresses.

» 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 Remote Address /URL corresponds to the IP address of the computer on which the Xesar software is operated. It is responsible for the communication between the Xesar network adapter and the Xesar software.
  It is important that the remote port (9081 by default) is the same as that specified in the Xesar Installation Manager (OCH Port).

The Remote IP (PC) and IP address (Xesar network adapter) are different! They must reside on the same network.

Sample configuration:

IP address	192.168.1.100
Subnet mask	255.255.255.0
Device Name	Adapter1
Login password	passwordadapater1
Remote IP	192.168.1.11

28.6 Resetting a network adapter

If you have forgotten your set password or the Xesar network adapter does not work due to incorrect input data, you can reset the Xesar network adapter to the factory settings.

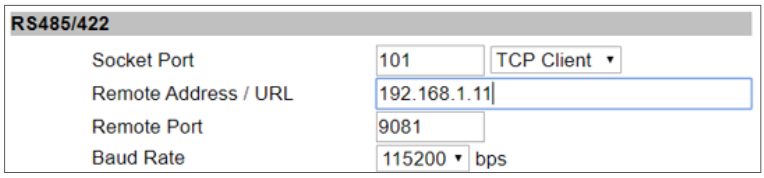
» Connect the mains adapter to the Xesar network adapter.

» Press the reset button for at least 5 seconds.

The password and settings are reset to the factory defaults.

» If you perform a reset of the Xesar network adapter in the event of an error, check the **parameter settings** again afterwards.

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



29 PC system: offline/online operation

29.1 System in offline operation

Access to your facility is enabled according to the authorisations defined on the access media. The Xesar software does not need to be running for the system to operate.

If you wish to make changes to your system, you must start the Xesar software and open the Xesar dashboard.

Changes, such as changes to authorisations for persons or access media, changes to components or changes to the system settings can only be carried out while the Xesar software is running.

29.1.1 Launch Xesar software

» Click the **Installation Manager button** on your desktop.
The Installation Manager starts and the Start window is displayed.

» In the start window, click on the **start button** of the desired system.
The system is started and the dashboard button is activated.

With the start of the system, the connected coding station is also activated and is ready to manage the access medium. (This only applies to the administrator PC; for client PCs with a coding station it is necessary to install and use the Periphery Manager).

» Click on the **activated dashboard button**
to go to the system login page.

» Log in with your **user name** and **password**.

After successful login, you can manage the installation according to your user rights using the Xesar dashboard.

29.1.2 Exit Xesar software

» Click the **Exit button**.
To stop the Xesar software, first close the system window in the browser by clicking the Exit button.

» Close the browser login window.

» Switch to the Installation Manager start window.

» Click the **stop button when the system is running**.

If you have selected "When stopping the system" in the system backup settings, this backup is carried out before stopping.

You can recognise a stopped installation in the start window of the Installation Manager when the start button is displayed.

Only one system can be started and run at a time.
If more than one system is managed in the Installation Manager, all start buttons of the other systems are deactivated as soon as one system is running.

When operating offline, the dashboard does not display current accesses or the current security status of the system. These functions are only accessible when the access system is in online mode.

29.2 System in online operation

If you operate your system online, the Installation Manager must be running and the system started.

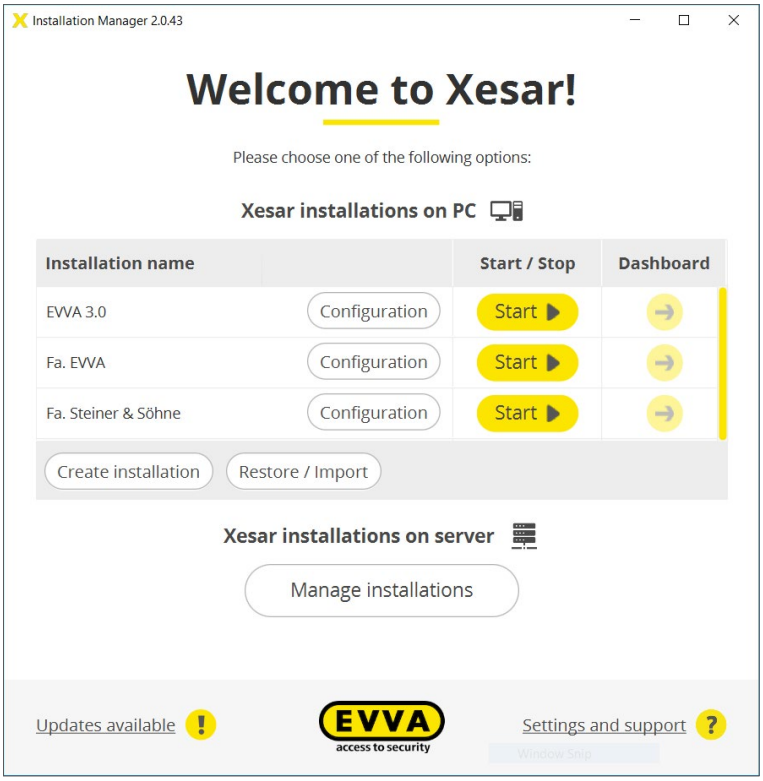
In online mode, you can monitor the current accesses and the current security status of the system and display them on the dashboard. This requires that the system be operated in online mode with XVN and with at least one online wall reader.

Persons only have access to the system in accordance with the authorisations defined on the access media.

Changes, such as authorisation changes for persons or access media, or component changes or changes in system settings, can be made at any time on the dashboard when the Xesar software is running.

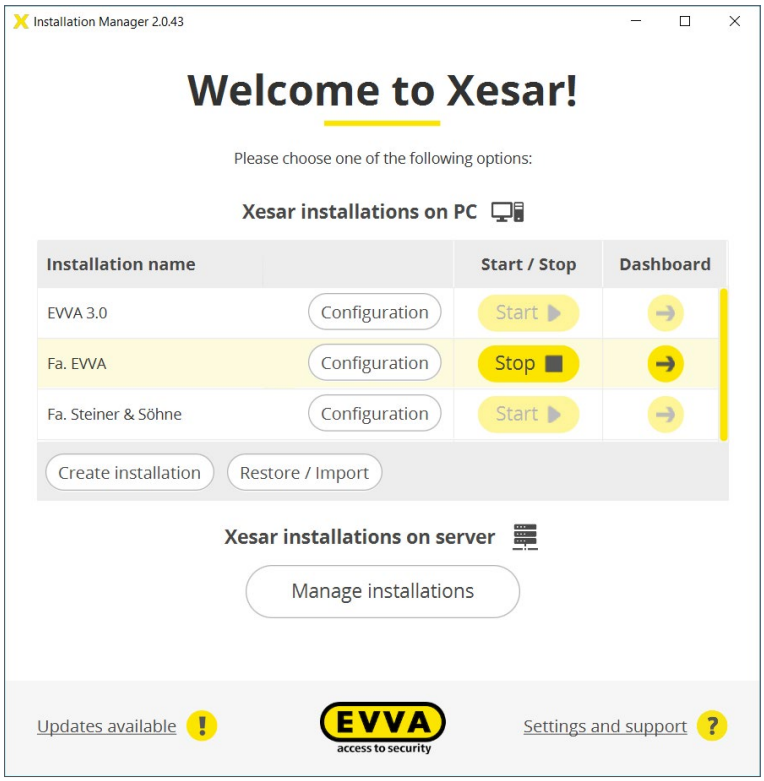
29.2.1 Launch Xesar software

» Click the **Installation Manager button** on your desktop.
The Installation Manager starts and the Start window is displayed.



» Click on the **start button**
in the start window. The desired system is started and the dashboard button is activated.

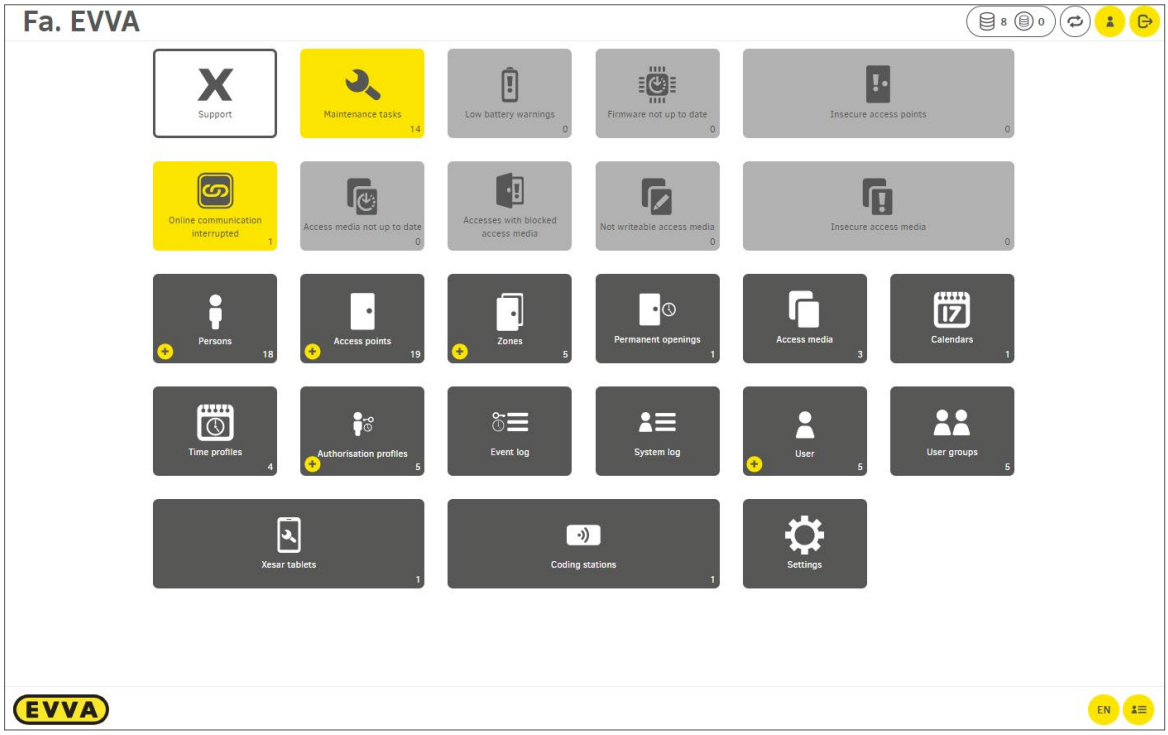
With the start of the system, the connected coding station is also activated and is ready to manage the access medium. (This only applies to the administrator PC; for client PCs with a coding station it is necessary to install and use the Periphery Manager).



» Click on the **activated dashboard button.**
You will be taken to the system login page.

» Log in with your **user name** and **password**.

After successful login, you can manage the system according to your user rights on the system dashboard.



29.2.2 Exit Xesar software

» Click the **Exit button** .
To stop the Xesar software, first close the system window in the browser by clicking the Exit button.

» Close the browser login window.

» Switch to the Installation Manager start window.

» Click the **stop button when the system is running**.

If you have selected “When stopping the system” in the system backup settings, this backup is carried out before stopping.

You can recognise a stopped installation in the start window of the Installation Manager when the start button is displayed.

Only one system can be started and run at one time.
If more than one system is managed in the Installation Manager, all start buttons of the other systems are deactivated as soon as one system is in operation.

When operating offline, the dashboard does not display current accesses or the current security status of the system. These functions are only accessible when the access system is in online mode.

29.3 PC system in multi-user operation

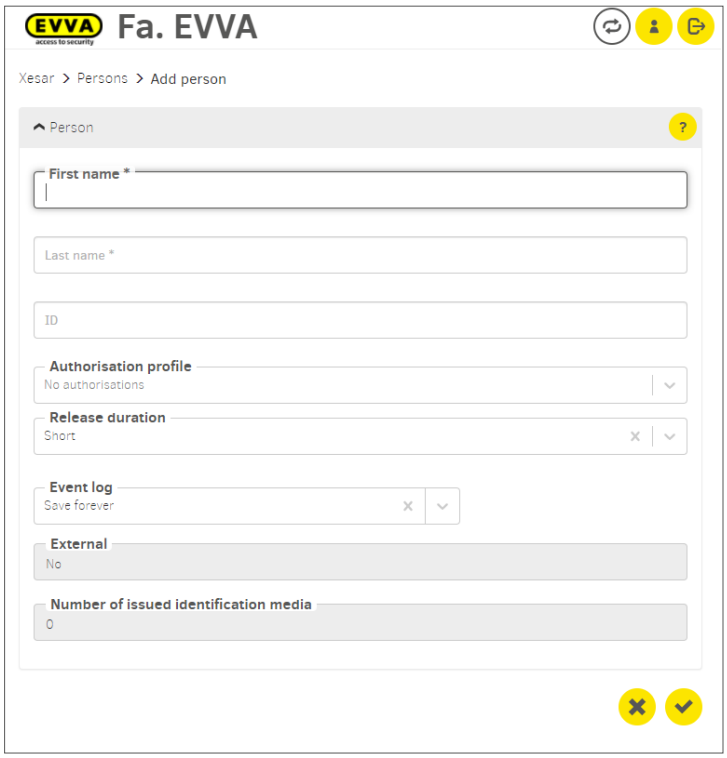
PC systems can also be managed in multi-user operation. To do this, the client PCs must be in the same network as the administrator PC (PC with Xesar software installed) and connect to the administrator PC via the IP address and port in the browser. After successful login, the client PCs can manage and operate the system.

An external coding station is required to manage access media on a client PC. To operate the coding station, the Periphery Manager must be installed, started and activated in the active browser window.

30 Xesar quick guide

30.1 Add person

A new employee has joined your company



- Select the **Personstile**.
- Click the **Plus icon.**
- Mandatory fields* must be filled in (first and last name).
- Enter ID (e.g. personnel number).

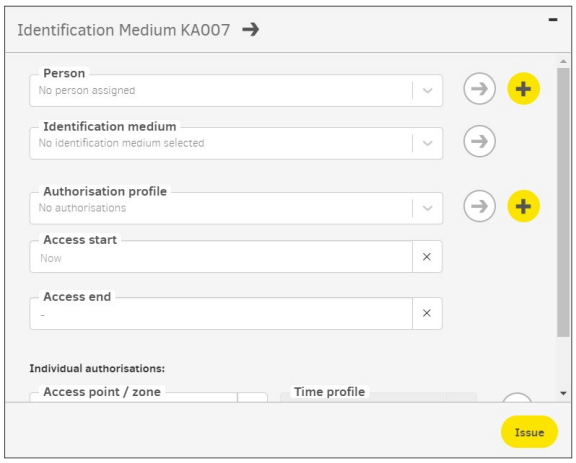
Optional convenience functions

- Release duration:
  Short/long (e.g. for persons with disabilities)
- Event log:
  Do not save / Save for a limited time / Save indefinitely
- If desired, already defined authorisations (authorisation profiles) can be selected for newly created persons.
- Individual authorisations are assigned later with the access medium.

If required, you can assign several access media to a person.

30.2 Issue access medium

To issue a new access medium, place it on the coding station. A pop-up window opens. You can optionally assign an identification number (ID).




Xesar

Issuing protocol

Installation name:	Fa. EVVA	
Person first name:	David	
Person last name:	Gruber	
ID person:	NA001	
ID identification medium:	KA001	
Release duration:	Short	
Event log:	Save forever	
Period logging:	—	
Authorisation interval:	15/03/2021 14:25 - ∞	
Validity duration:	14 days	
Authorisation profile:	Büro	
All authorisations:	Access points	Time profile
	Eingang 2	—
	Eingang 1	—
	Zones	Time profile
	Büros	—
Individual authorisations:	Access point / zone	Time profile
Date issued:	15/03/2021 16:26	
Issuing user:	Helmut	

Issuance:

Signature

Revocation:

Signature

EVVA access to security

Access media do not necessarily have to be assigned to a person. This is ideal for access by external companies with changing staff.

- **Optional:** Select a person in the access medium.
- Select an authorisation profile.
- **If you want to restrict the authorisation period**, change the authorisation start and end in the access medium.
- **Optional:** Select individual access to specific installation locations, e.g. Wardrobe locker.
- Issue the access medium.

An event log is created with the data at the time of output.

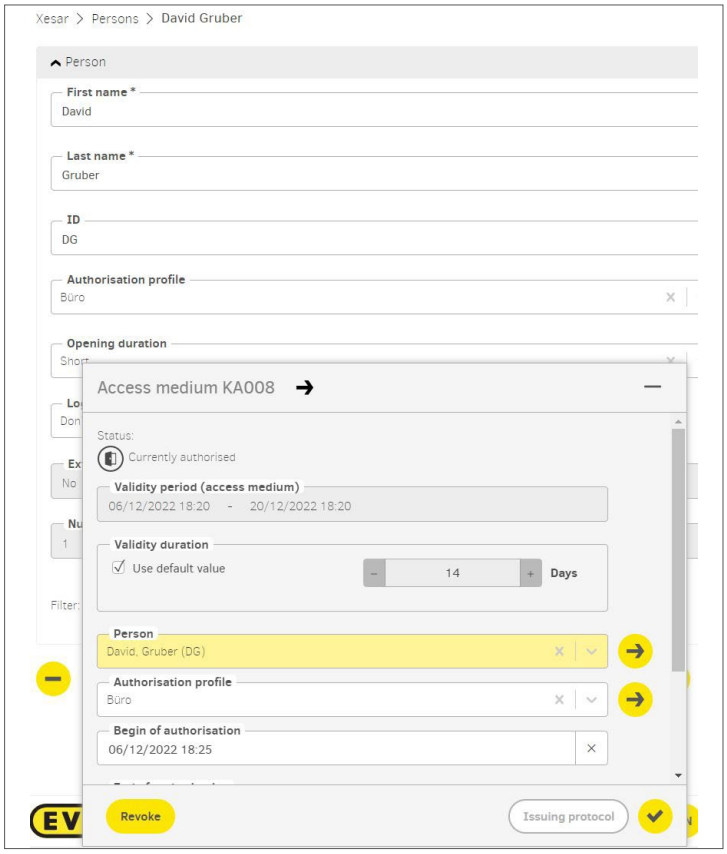
- Print out the event log and have the assigned person confirm that the access medium has been transferred.

The withdrawal of the access medium can be confirmed in the event log.

If required, you can assign several access media to a person.

If you are using the KeyCredits payment model, click the Debit button  , to confirm the authorisation change.
The KeyCredit Xesar Lifetime payment model includes new access media and authorisation changes.

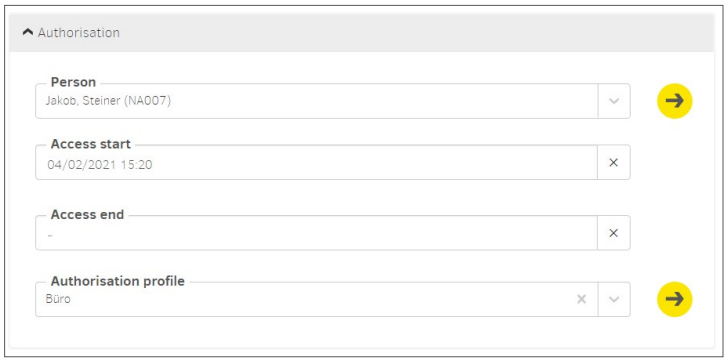
30.3 Simple method: Assign access media to a person



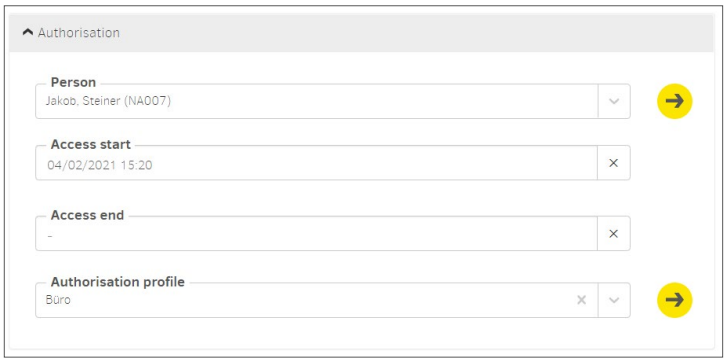
- Open the person details page of the desired person.
- Place a new Xesar access medium on the coding station.
- The name of the person with the authorisation profile is automatically inserted in the overlay window.
- Confirm the entry in the overlay window.
- If necessary, an output log can be created.

30.4 Change, add or delete authorisation profiles

An employee moves to another department and needs a corresponding authorisation profile:



- Click on the dashboard tile **Access Media**:
  Authorisation profiles and individual authorisations for access media can be selected and changed under the dashboard tile “Access Media” in the respective access media detail view.
- After making changes, place the access medium on the coding station to update the access medium.



- Authorisation profiles and individual authorisations can also be selected or changed directly by placing the access medium on the coding station displayed in the window.

Special case: Fire service and general master key
If necessary, a general master key or fire service authorisation profile can be assigned to an access medium.

An access medium with a **fire brigade authorisation profile** has access to every door in your system **for an unlimited period of time**.
An access medim with **a general master key authorisation profile** has access to every door in your system and **can be limited in its period of validity**. After the validity period has expired, the access medium must be updated again.

Store access media with fire service or general master key authorisation particularly securely and carefully.

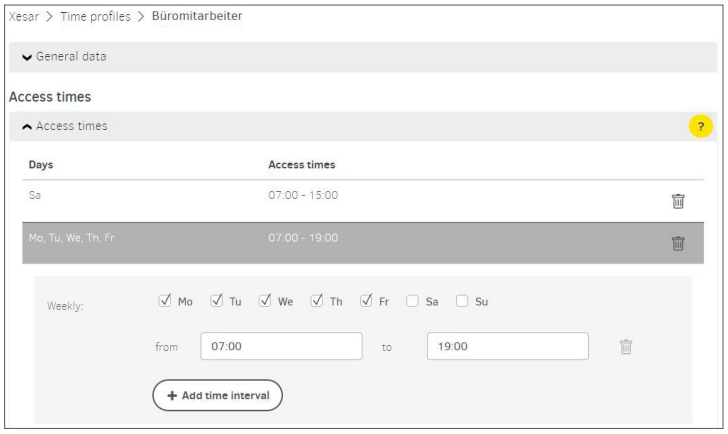
In a single system, a maximum of 15 media can be issued with a fire brigade or general master key authorisation profile.

A detailed description on the subject of “authorisation profiles” can be found in the Xesar system manual.

30.5 Changing time profiles

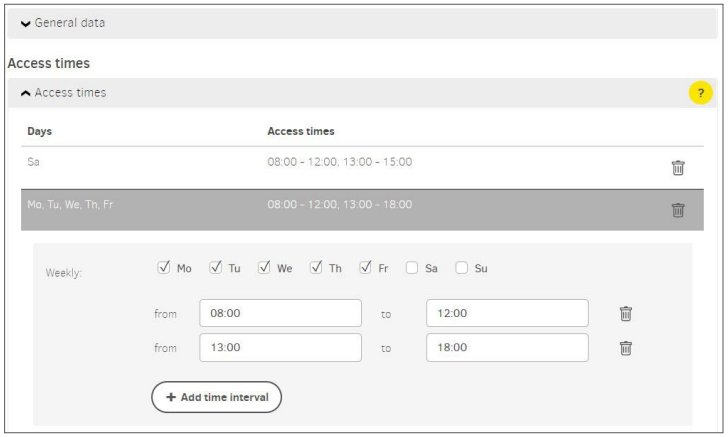
A person receives access authorisations with amended times.
The opening hours of the salesroom have changed.

Time profile:



» Change time windows for access
If the working time for a person or a group of persons changes, the time windows for the access of the person or group of persons must be changed.

Office mode time profile



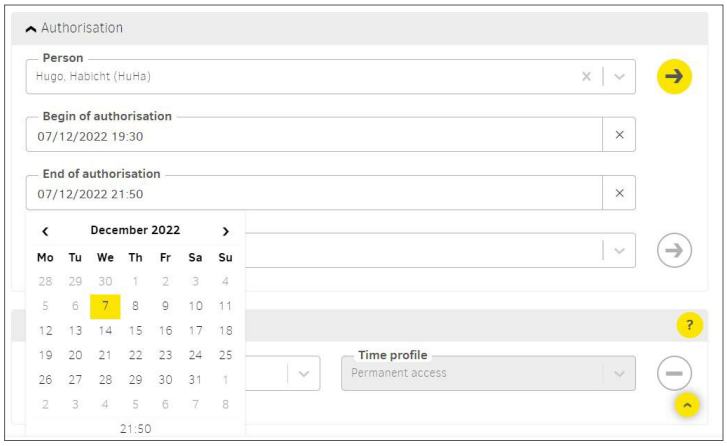
» At a certain point in time, a component is to switch to continuous open mode and then close at a certain point in time.

A detailed description on the topic of “time profiles” can be found in the Xesar system manual.

The times in the input fields can be entered numerically or using the arrow keys.

30.6 Deactivate access media

The access medium can be deactivated if a person's access authorisation is to be suspended for an extended period of time. The medium with the authorisation profile remains allocated to the person. Access is deactivated until further notice by setting the end of authorisation to the current time.



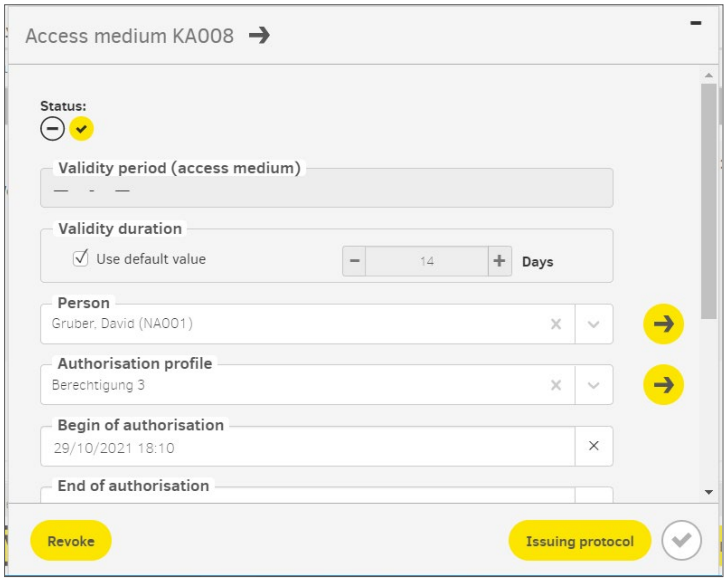
» Open the detail page of the access medium to be deactivated.
» Click on the currently active end of authorisation (date and time, e.g. 7.12 at 21:35). The medium is immediately deactivated.
» Then update the medium at the online wall reader or coding station so that it no longer has access to the system.

The access authorisation can be reactivated on the medium by setting a new authorisation end time and then updating it at the online wall reader or at the coding station.

No blacklist entries are generated in the system during this process.

30.7 Withdrawal of access medium

Withdraw an access medium and reuse it in the facility at a later time, e.g. after an employee leaves the company.



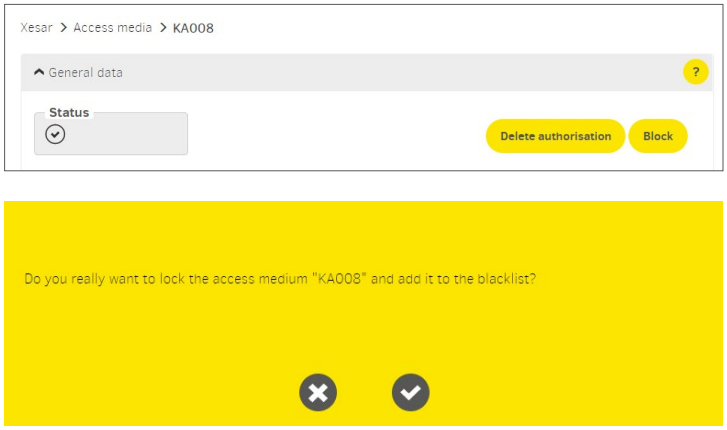
» Place the access medium on the coding station.
» Select **withdraw**.

After being withdrawn, the access medium can only be reused in this system and will be displayed as a new access medium after being placed on the coding station again.

You will find a detailed description on the subject of "withdrawing of medium" in the Xesar system manual.

30.8 Block access medium

An access medium has been lost or stolen.
In order to protect the system from unauthorised access, the access medium must be blocked.



30.8.1 Block access medium

- Select the **access medium**tile.
- Select the access medium to be blocked and click **Block**.

The Xesar software generates a blacklist and maintenance tasks for all components of vulnerable installation locations.

- Synchronise the Xesar tablet and perform maintenance tasks on the components.
- Alternatively, the blacklist can be distributed to the components using access media.
- Delete key function – the blocked access medium is permanently deactivated on synchronised Xesar devices with the current blacklist.

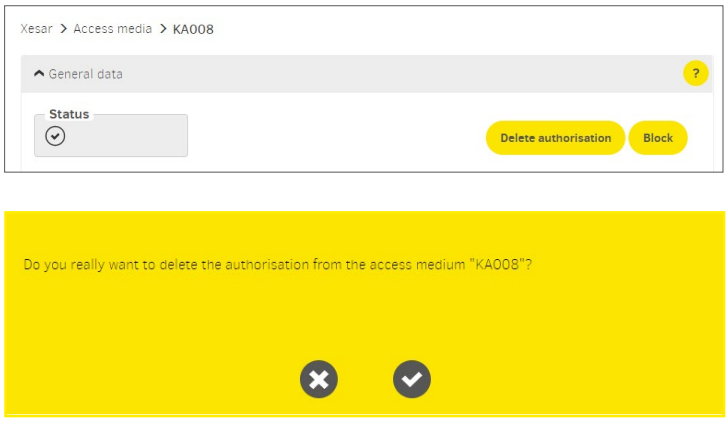
30.8.2 Delete authorisations

Authorisations can be withdrawn from an existing access medium.

- Authorisations on the access medium are deleted.
- No blacklist entry and no maintenance tasks are generated.
- The access medium remains assigned to the person.
- New authorisations can be assigned.

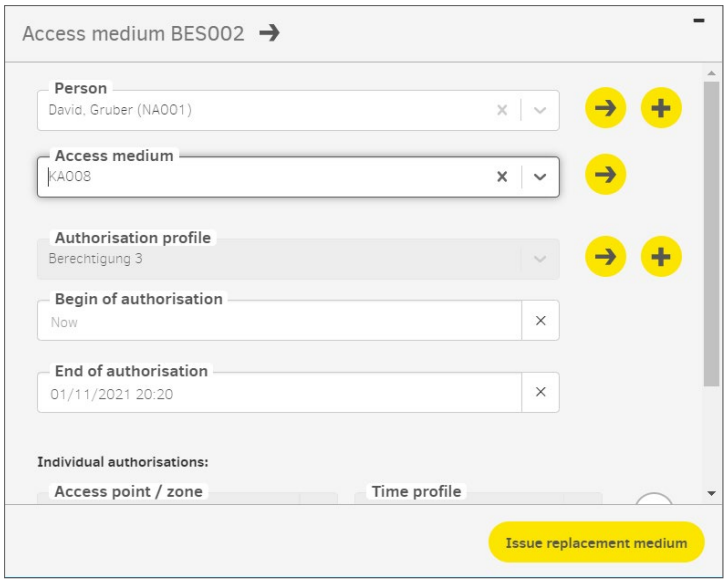
» **Update access medium**
To update, the access medium must be held on the online wall reader or placed on the coding station.

A detailed description on the subject of “Locking an access medium” can be found in the Xesar system manual.



30.9 Assigning replacement medium

The user has left the personal Xesar identification medium at home – create a replacement medium.



- Place a new Xesar identification medium on the coding station.
- In the "Person" drop-down field, select the person for whom you would like to issue a replacement medium.
- Select the access medium to be replaced in the "Access medium" drop-down field.
- Click on **Assign replacement medium**.

The replacement medium now has the authorisations of the original medium for the set authorisation duration.

- The authorisation period for replacement media can be set under the **settings** tile in the Xesar software.

Please note that the original medium remains valid.

For help and further information, please contact your EVVA partner or the EVVA technical office.

Refer to our Xesar system manual for a detailed description of the "Issuing replacement medium" process.

www.evva.com