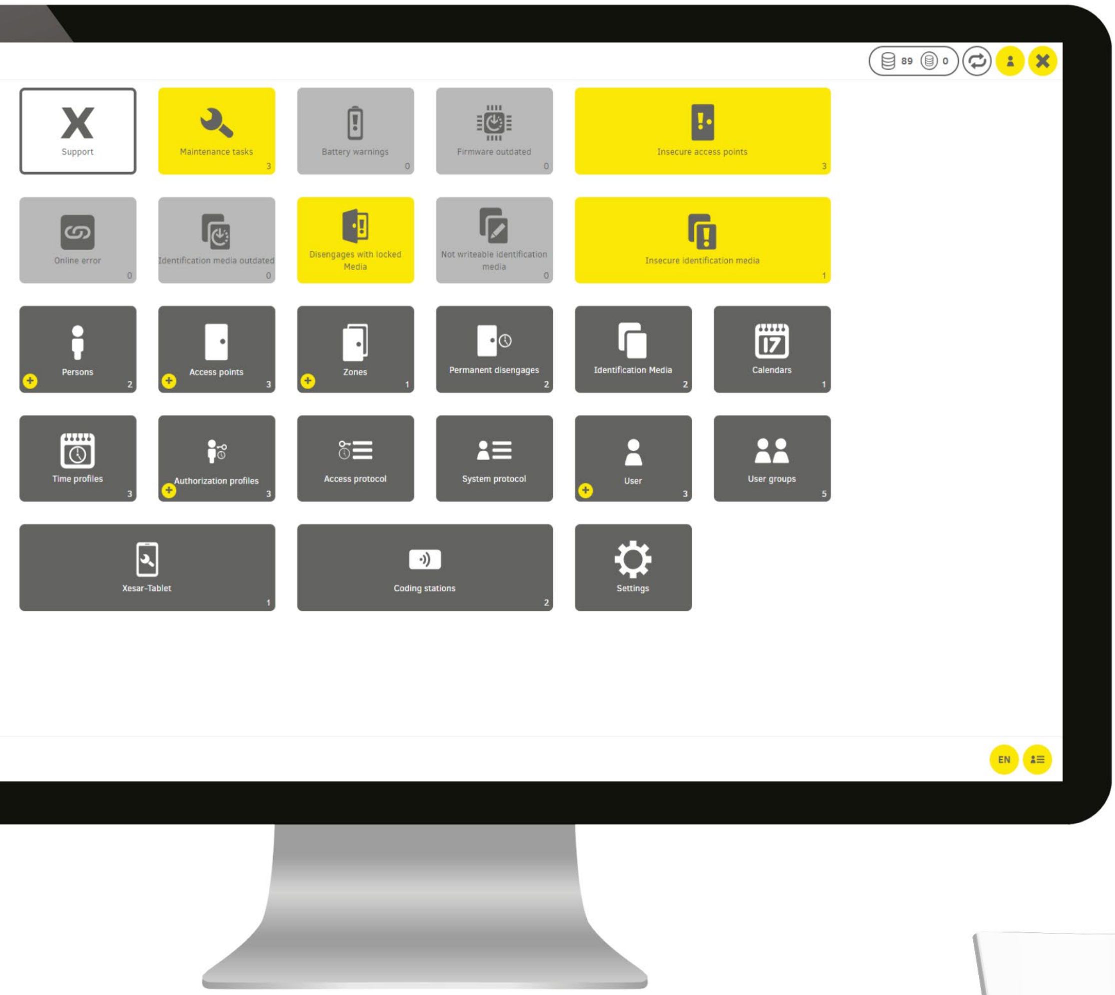
EVVA
access to security



Xesar

Commissioning Xesar software

Imprint

Product code: I.X.R3-2.AN.INB.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 document is an excerpt from the Xesar 3.1 system manual.

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

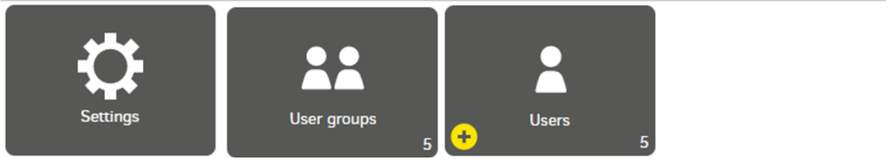
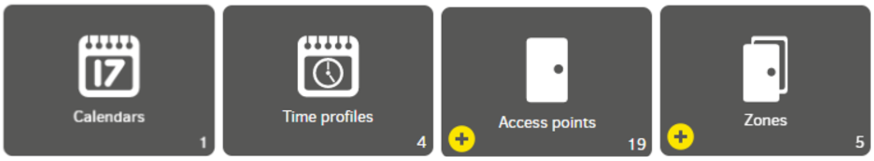
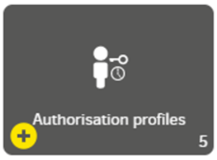
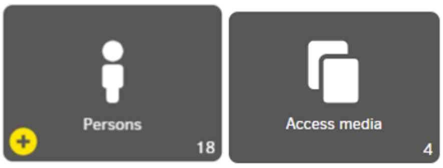
#	Status	Symbol	Explanation
13	Not updated / waiting for update / download of update	⚠	An update is available and can be downloaded
14	Search	🔍	Search for a specific event contribution
15	Maximise	⌄	Extending the Field of View
16	Minimise	⌃	Reduce the field of view
17	Go to	→	Open the browser window 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	DE	Change language
25	Show KeyCredit units	0 0	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	csv xls	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	Backup	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	ᛒ	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	ᛒ	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 Commissioning Xesar software

1st Step	
2nd Step	 Calendars 1 Time profiles 4 Access points 19 Zones 5
3rd Step	
4th Step	

2.1 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.

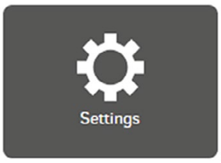
Mandatory fields are marked *****.

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

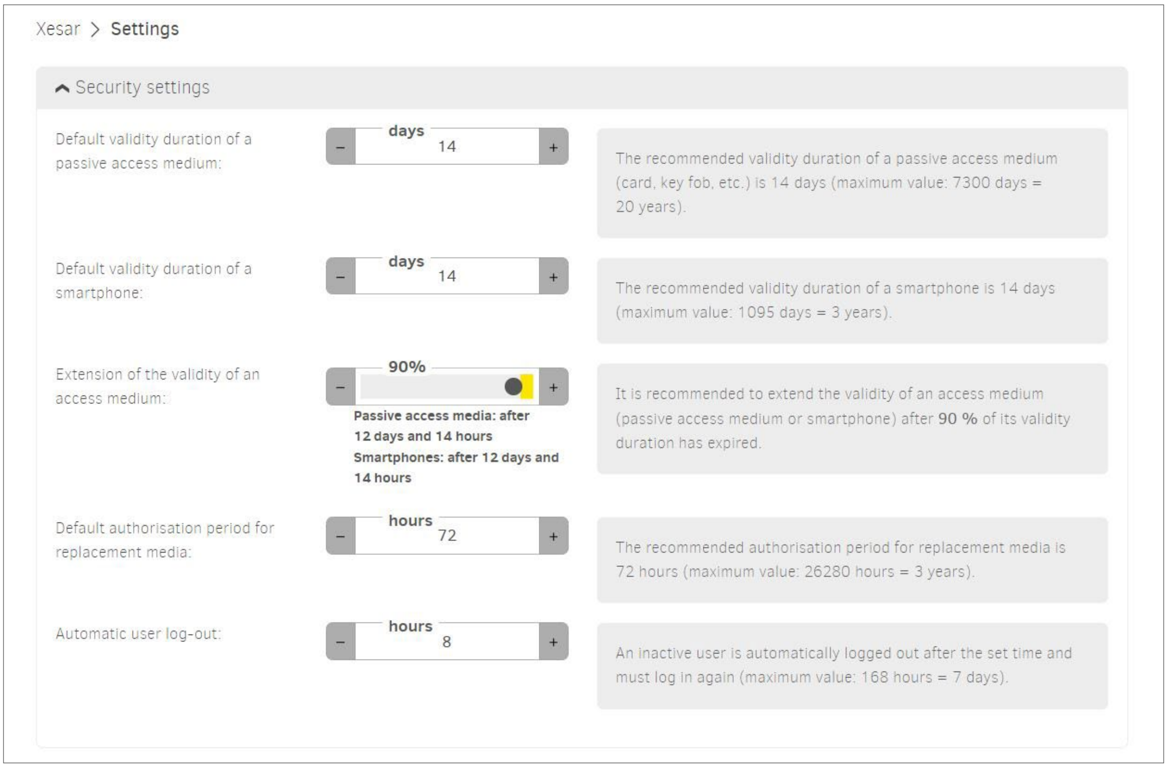
Double-clicking on the column divider adjusts the column width to the column header.

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

2.2 Settings



2.2.1 Security settings



Xesar > Settings

Security settings

Default validity duration of a passive access medium: days 14

The recommended validity duration of a passive access medium (card, key fob, etc.) is 14 days (maximum value: 7300 days = 20 years).

Default validity duration of a smartphone: days 14

The recommended validity duration of a smartphone is 14 days (maximum value: 1095 days = 3 years).

Extension of the validity of an access medium: 90%

Passive access media: after 12 days and 14 hours
Smartphones: after 12 days and 14 hours

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

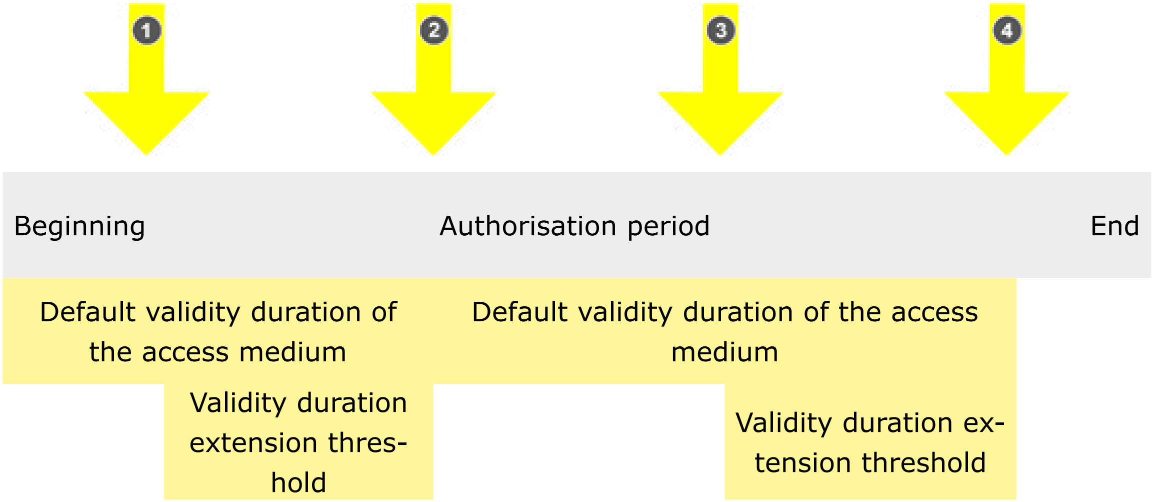
Default authorisation period for replacement media: hours 72

The recommended authorisation period for replacement media is 72 hours (maximum value: 26280 hours = 3 years).

Automatic user log-out: hours 8

An inactive user is automatically logged out after the set time and must log in again (maximum value: 168 hours = 7 days).

2.2.2 Validity duration and authorisation period of the access media


1
2
3
4
Beginning
Authorisation period
End
Default validity duration of the access medium
Default validity duration of the access medium
Validity duration extension threshold
Validity duration extension threshold

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.

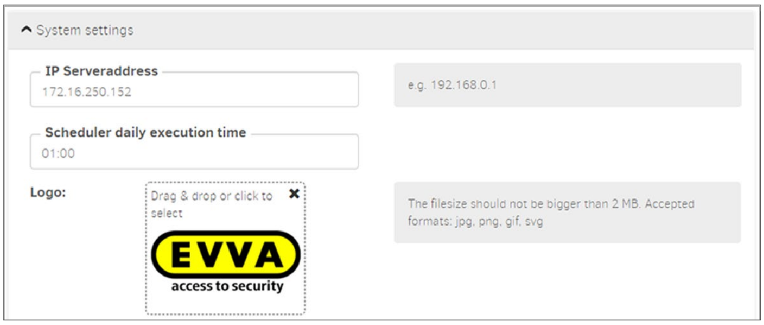
Default authorisation period for replacement media:

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.

2.2.3 System settings



System settings

IP Serveraddress: 172.16.250.152

e.g. 192.168.0.1

Scheduler daily execution time: 01:00

Logo:

The filesize should not be bigger than 2 MB. Accepted formats: jpg, png, gif, svg

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:

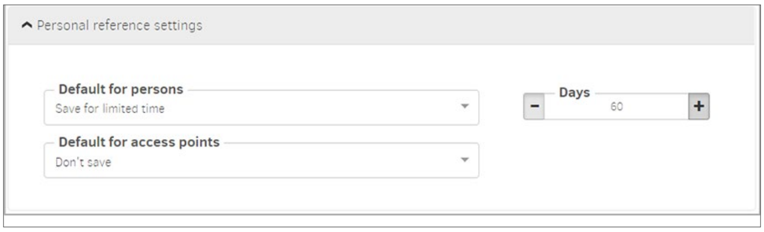
The logo is displayed on the dashboard in front of the names of the installations. If you want to add a custom logo, please note the following specifications:

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.



Personal reference settings

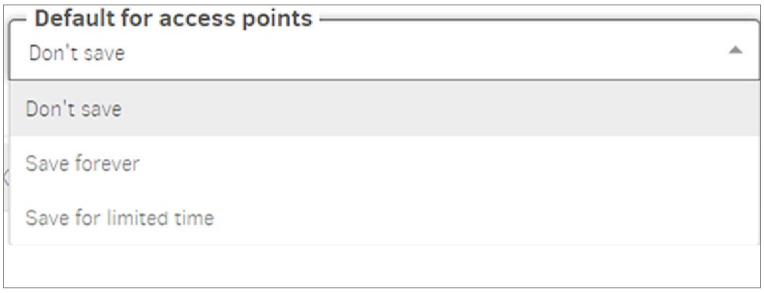
Default for persons: Save for limited time

Days: 60

Default for access points: Don't save

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

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



Default for access points: Don't save

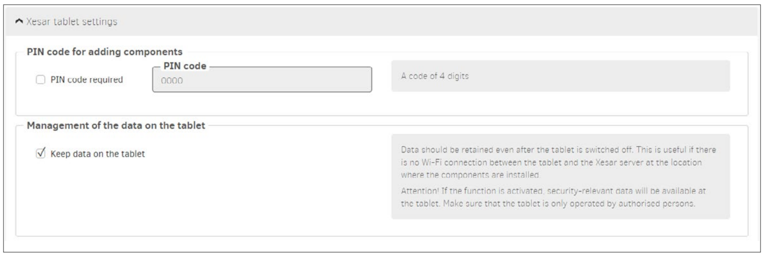
Person and component-specific settings are defined in the tiles “Persons” or “Access points – Component”.

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.



Xesar tablet settings

PIN code for adding components

□ PIN code required

PIN code: 0000

A code of 4 digits

Management of the data on the tablet

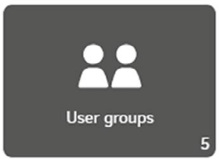
☑ Keep data on the tablet

Data should be retained even after the tablet is switched off. This is useful if there is no Wi-Fi connection between the tablet and the Xesar server at the location where the components are installed.

Attention! If the function is activated, security-relevant data will be available at the tablet. Make sure that the tablet is only operated by authorised persons.

2.3 User groups:

The authorisations for users are defined within the user groups.



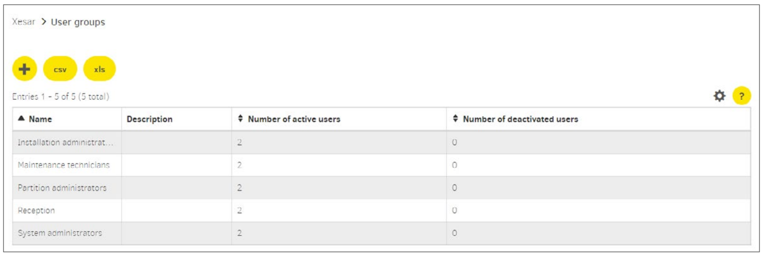
Users manage the system using the Xesar software. Any number of users can be created with various authorisations (depending on their function). These different authorisations are defined in the user groups.

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.



Entries 1 - 5 of 5 (5 total)

▲ Name	Description	⇕ Number of active users	⇕ Number of deactivated users
Installation administrat…		2	0
Maintenance technicians		2	0
Partition administrators		2	0
Reception		2	0
System administrators		2	0

The following predefined user groups are available for selection:

System administrator
may modify user passwords

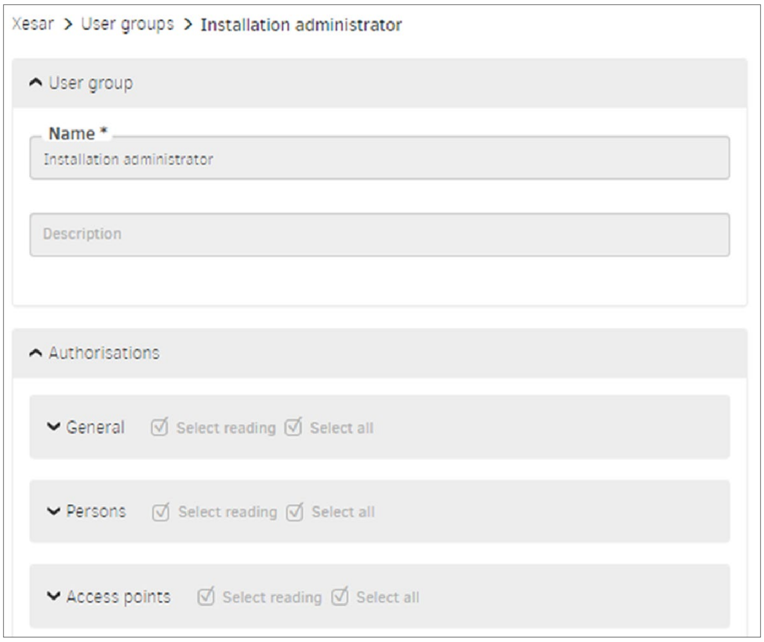
Installation manager
has all authorisations but may not change user passwords

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:



Xesar > User groups > Installation administrator

User group

Name *
Installation administrator

Description

Authorisations

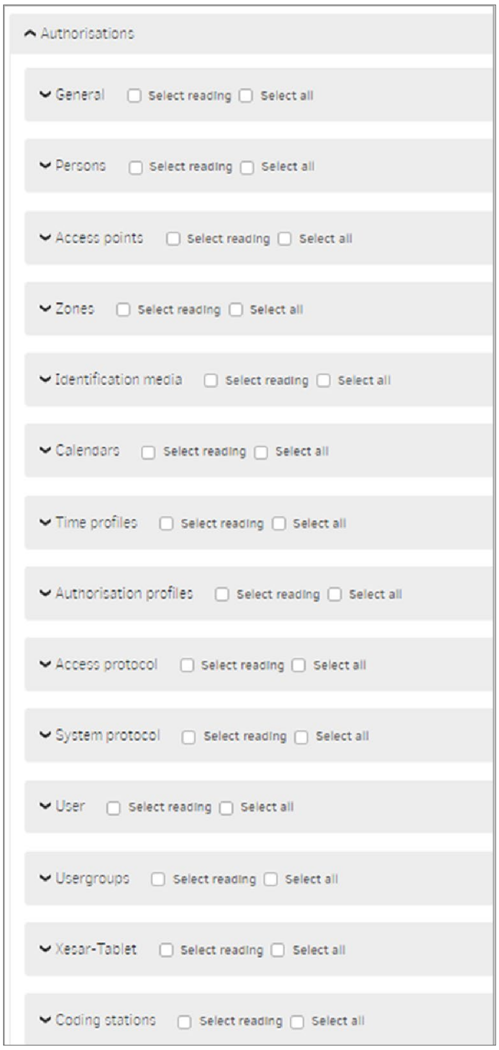
General ☑ Select reading ☑ Select all

Persons ☑ Select reading ☑ Select all

Access points ☑ Select reading ☑ Select all

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.



Authorisations

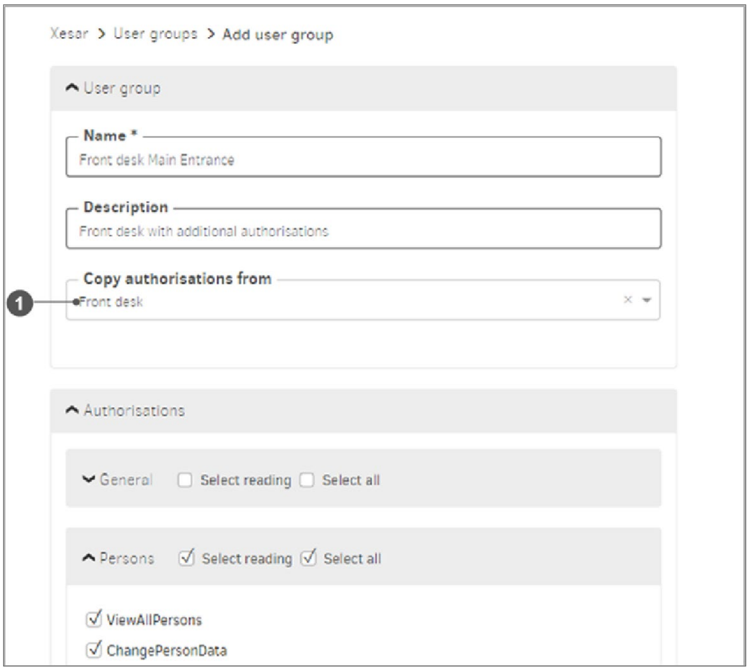
General	□ Select reading	□ Select all
Persons	□ Select reading	□ Select all
Access points	□ Select reading	□ Select all
Zones	□ Select reading	□ Select all
Identification media	□ Select reading	□ Select all
Calendars	□ Select reading	□ Select all
Time profiles	□ Select reading	□ Select all
Authorisation profiles	□ Select reading	□ Select all
Access protocol	□ Select reading	□ Select all
System protocol	□ Select reading	□ Select all
User	□ Select reading	□ Select all
Usergroups	□ Select reading	□ Select all
Xesar-Tablet	□ Select reading	□ Select all
Coding stations	□ Select reading	□ Select all

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:



Xesar > User groups > Add user group

User group

Name *: Front desk Main Entrance

Description: Front desk with additional authorisations

Copy authorisations from: Front desk

Authorisations

General ☐ Select reading ☐ Select all

Persons ☑ Select reading ☑ Select all

☑ ViewAllPersons

☑ ChangePersonData

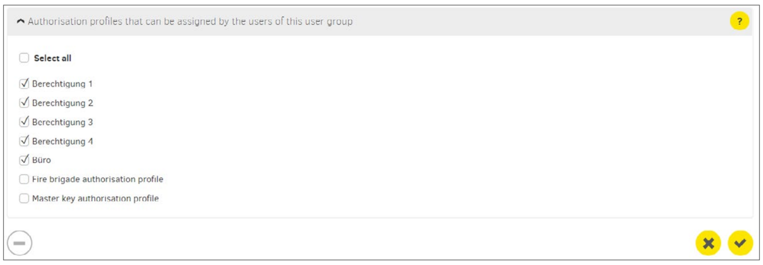
Use the predefined user groups as the basis for assigning authorisations to users.

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.

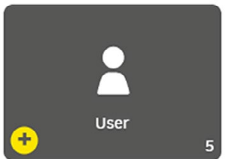


Authorisation profiles that can be assigned by the users of this user group

□ **Select all**

☑ Berechtigung 1
☑ Berechtigung 2
☑ Berechtigung 3
☑ Berechtigung 4
☑ Büro
□ Fire brigade authorisation profile
□ Master key authorisation profile

2.4 Users



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

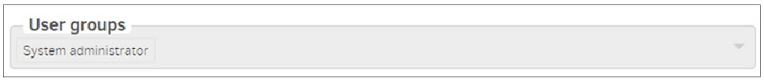
A new user can be added using the '**Add**' icon. The number of registered users is displayed in the User tile.

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.

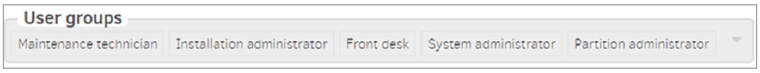
The users **su** (super administrator) and **admin** (administrator) that were created during the initial installation cannot be changed or deleted.

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

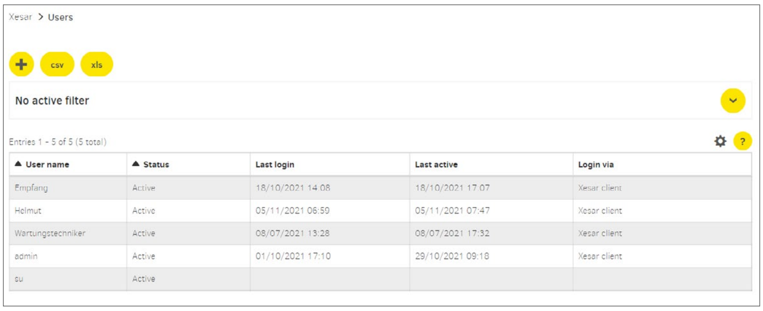


User groups: System administrator

- **admin**
  has all rights



User groups: Maintenance technician, Installation administrator, Front desk, System administrator, Partition administrator



Xesar > Users

No active filter

Entries 1 - 5 of 5 (5 total)

▲ User name	▲ Status	Last login	Last active	Login via
Empfang	Active	18/10/2021 14:08	18/10/2021 17:07	Xesar client
Helmut	Active	05/11/2021 06:59	05/11/2021 07:47	Xesar client
Wartungstechniker	Active	08/07/2021 13:28	08/07/2021 17:32	Xesar client
admin	Active	01/10/2021 17:10	29/10/2021 09:18	Xesar client
su	Active			

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.

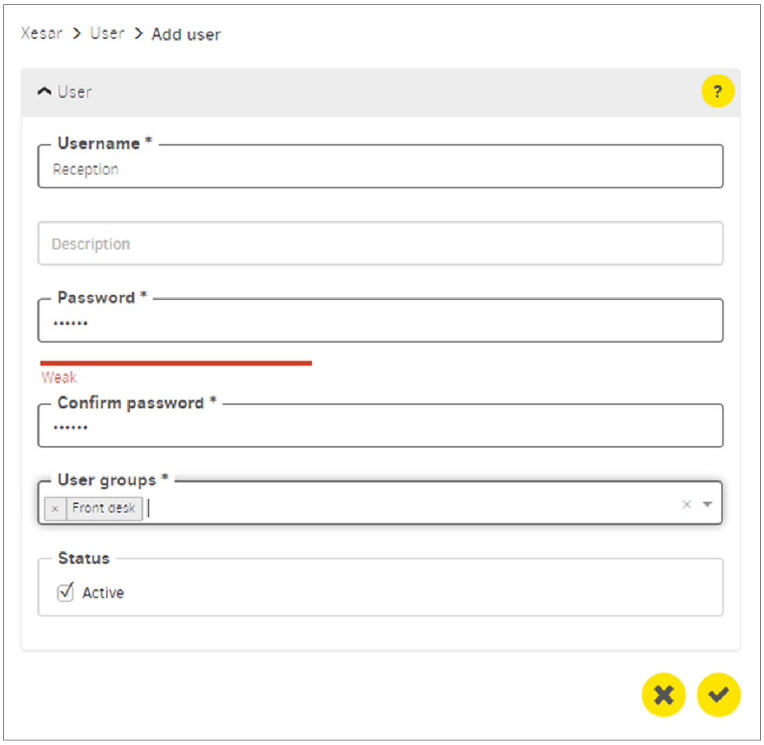
User groups
Selection of the user groups defined for the user. At least one user group must be selected.

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.



Xesar > User > Add user

User

Username *
Reception

Description

Password *
••••••

Weak

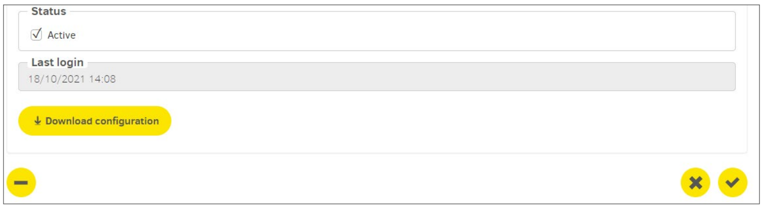
Confirm password *
••••••

User groups *
Front desk

Status
☑ Active

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).



Status
☑ Active

Last login
18/10/2021 14:08

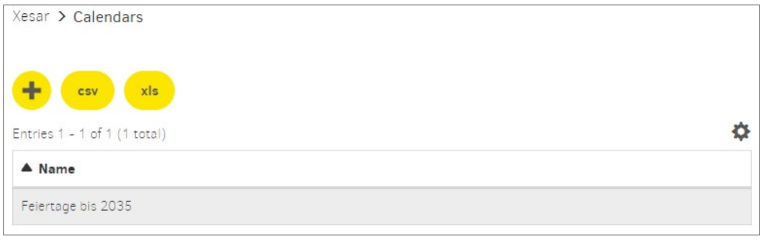
Download configuration

2.5 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.

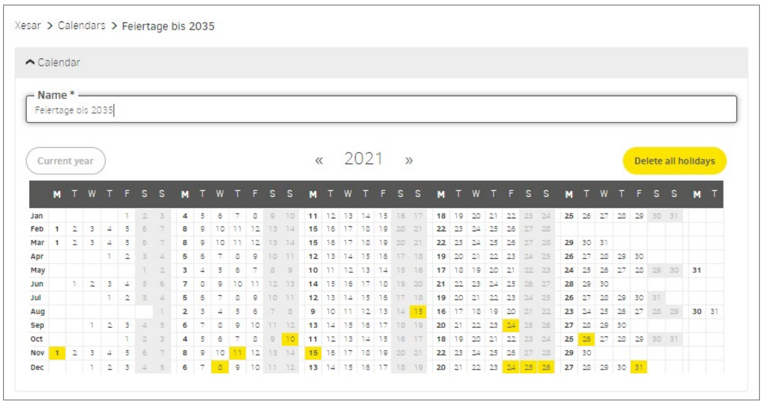
A holiday (e.g. Christmas) may only occur in one calendar.



Xesar > Calendars

Entries 1 - 1 of 1 (1 total)

▲ Name
Feiertage bis 2035



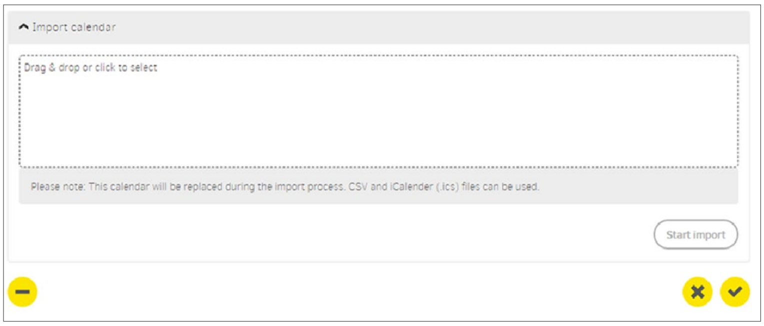
Xesar > Calendars > Feiertage bis 2035

Calendar

Name *: Feiertage bis 2035

Import calendar

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



Import calendar

Drag & drop or click to select

Please note: This calendar will be replaced during the import process. CSV and iCalender (.ics) files can be used.

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

2.6 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:

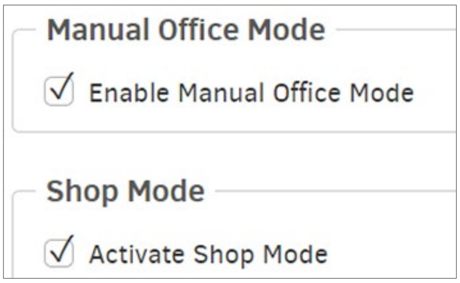
Within Xesar, manual office mode means the manual activation of a permanent release of Xesar access components. For the function, both the corresponding Xesar access component and the corresponding access medium must be authorised via the authorisation profile. Set the manual office mode in the respective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



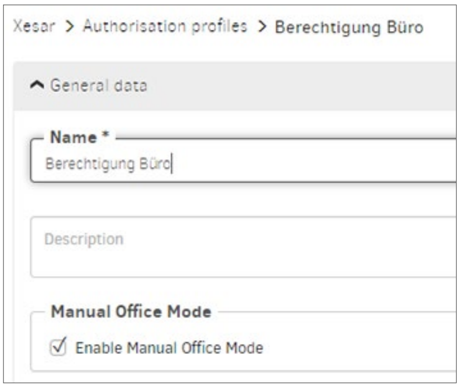
Manual Office Mode

☑ Enable Manual Office Mode

Shop Mode

☑ Activate Shop Mode

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



Xesar > Authorisation profiles > Berechtigung Büro

General data

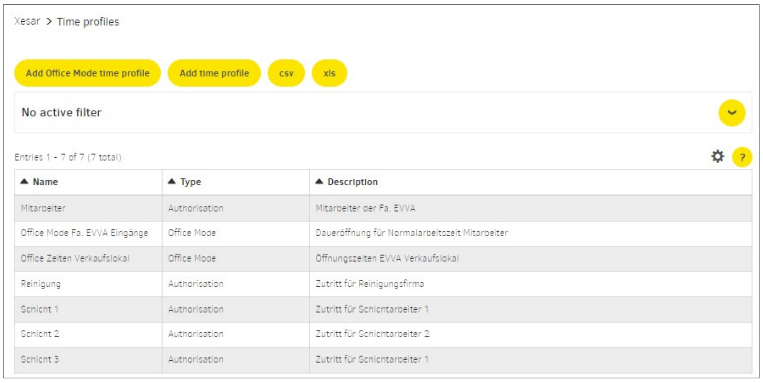
Name *: Berechtigung Büro

Description

Manual Office Mode

☑ Enable Manual Office Mode

Time profiles view:



Xesar > Time profiles

No active filter

Entries 1 - 7 of 7 (7 total)

Name	Type	Description
Mitarbeiter	Authorisation	Mitarbeiter der Fa. EVVA
Office Mode Fa. EVVA Eingänge	Office Mode	Daueröffnung für Normalarbeitszeit Mitarbeiter
Office Zeiten Verkaufslokal	Office Mode	Öffnungszeiten EVVA Verkaufslokal
Reinigung	Authorisation	Zutritt für Reinigungsfirma
Schicht 1	Authorisation	Zutritt für Schichtarbeiter 1
Schicht 2	Authorisation	Zutritt für Schichtarbeiter 2
Schicht 3	Authorisation	Zutritt für Schichtarbeiter 1

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

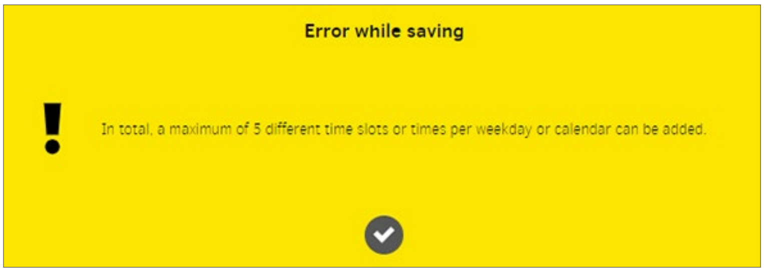
2.6.1 Add office mode time profile

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.

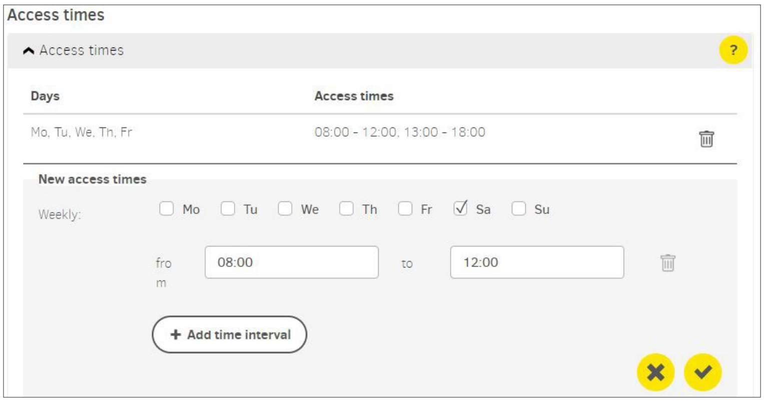
In total, a maximum of 5 different time slots or times per weekday or calendar can be added.



Error while saving

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.



Access times

Access times

Days	Access times
Mo, Tu, We, Th, Fr	08:00 - 12:00, 13:00 - 18:00

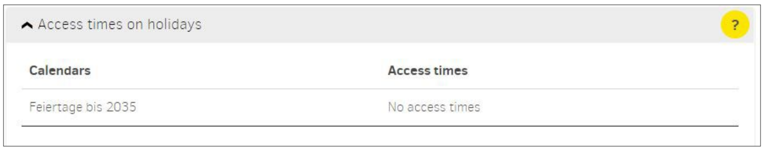
New access times

Weekly: ☐ Mo ☐ Tu ☐ We ☐ Th ☐ Fr ☑ Sa ☐ Su

from 08:00 to 12:00

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.



Access times on holidays

Calendars	Access times
Feiertage bis 2035	No access times

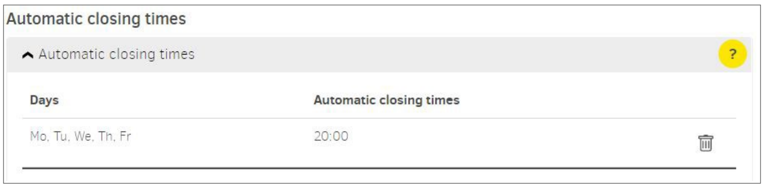
Automatic closing times:

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.

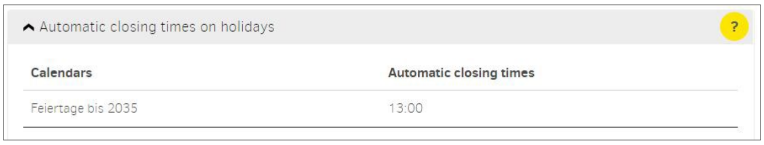
Example:
Closing time Monday to Friday, 8:00 pm each day


Automatic closing times

Days	Automatic closing times
Mo, Tu, We, Th, Fr	20:00

Automatic closing times on public holidays:

The closing time can be changed for holidays.



Calendars	Automatic closing times
Feiertage bis 2035	13:00

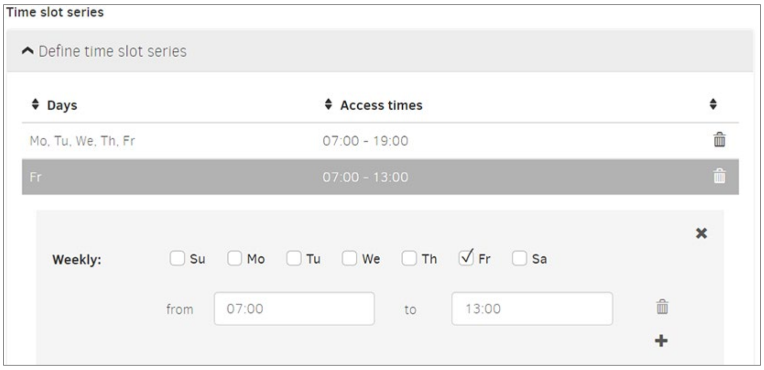
2.6.2 Adding a time profile

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 slot series

Define time slot series

Days	Access times
Mo, Tu, We, Th, Fr	07:00 - 19:00
Fr	07:00 - 13:00

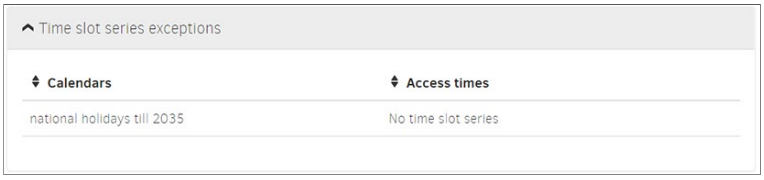
Weekly: □ Su □ Mo □ Tu □ We □ Th ☑ Fr □ Sa

from 07:00 to 13:00

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.

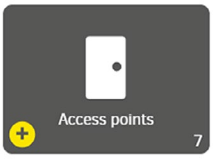
No time slot series means that there is no access on holidays defined in the calendar. All existing calendars are displayed.



Time slot series exceptions

Calendars	Access times
national holidays till 2035	No time slot series

2.7 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

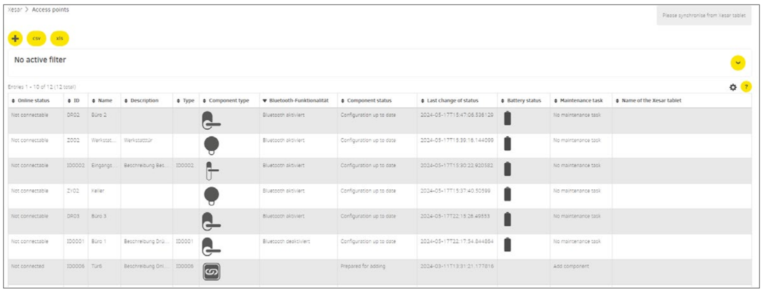
Life cycle status:
describes the current status of the component, e. g. prepared for adding

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



Xesar > Access points

Please synchronise from Xesar tablet

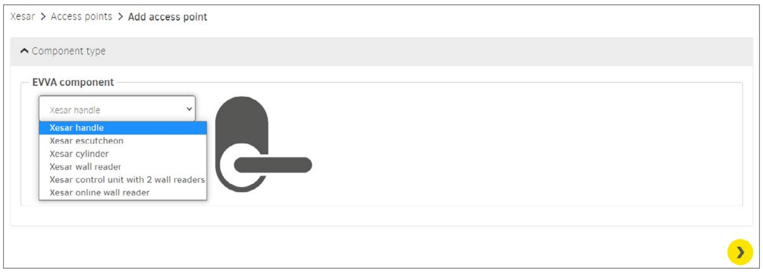
No active filter

Entries 1 - 10 of 12 (12 total)

Online status	ID	Name	Description	Type	Component type	Bluetooth-Funktionalität	Component status	Last change of status	Battery status	Maintenance task	Name of the Xesar tablet
Not connectable	DR02	Büro 2				Bluetooth aktiviert	Configuration up to date	2024-05-17T15:47:06.536129	▮	No maintenance task	
Not connectable	Z002	Werkstat...	Werkstatttür			Bluetooth aktiviert	Configuration up to date	2024-05-17T15:39:16.144099	▮	No maintenance task	
Not connectable	ID0002	Eingangs...	Beschreibung Bes...	ID0002		Bluetooth aktiviert	Configuration up to date	2024-05-17T15:30:22.920582	▮	No maintenance task	
Not connectable	ZY02	Keller				Bluetooth aktiviert	Configuration up to date	2024-05-17T15:37:40.50599	▮	No maintenance task	
Not connectable	DR03	Büro 3				Bluetooth aktiviert	Configuration up to date	2024-05-17T22:15:26.49553	▮	No maintenance task	
Not connectable	ID0001	Büro 1	Beschreibung Drü...	ID0001		Bluetooth deaktiviert	Configuration up to date	2024-05-17T22:17:54.844864	▮	No maintenance task	
Not connected	ID0006	Tür6	Beschreibung Onl...	ID0006			Prepared for adding	2024-03-11T13:31:21.177816		Add component	

2.7.1 Add access point

Select the desired access component.



Xesar > Access points > Add access point

Component type

EVVA component

2.7.2 Describe access point

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

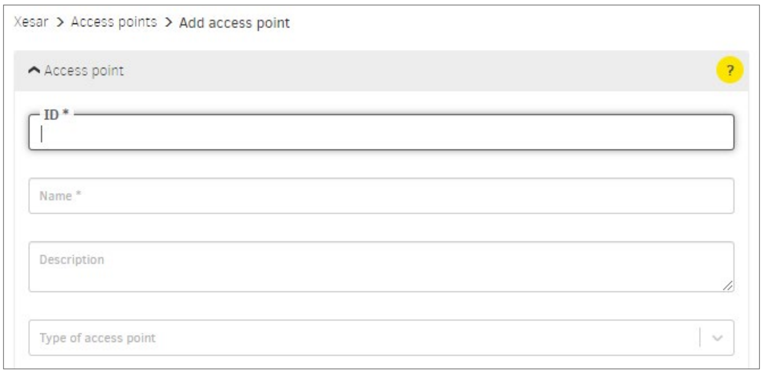
Mandatory fields are marked with *.

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



Xesar > Access points > Add access point

Access point

ID *

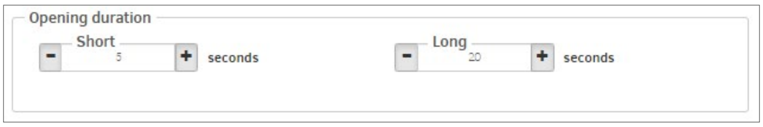
Name *

Description

Type of access point

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.



Opening duration

Short: 5 seconds

Long: 20 seconds

Time profile:
selection of the office time profile mode

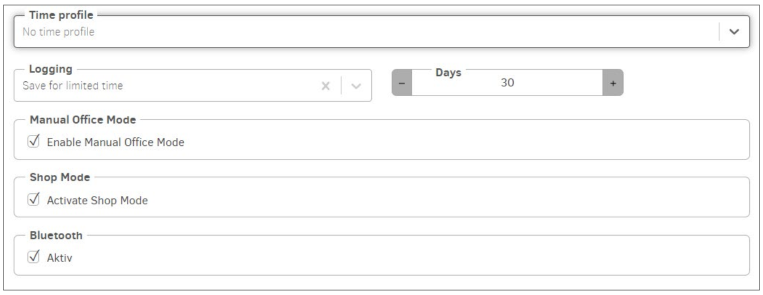
Logging:
definition of the access event recording type and the duration of data recording

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.



Time profile
No time profile

Logging
Save for limited time

Days
30

Manual Office Mode
☑ Enable Manual Office Mode

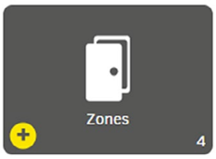
Shop Mode
☑ Activate Shop Mode

Bluetooth
☑ Aktiv

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.

2.8 Areas



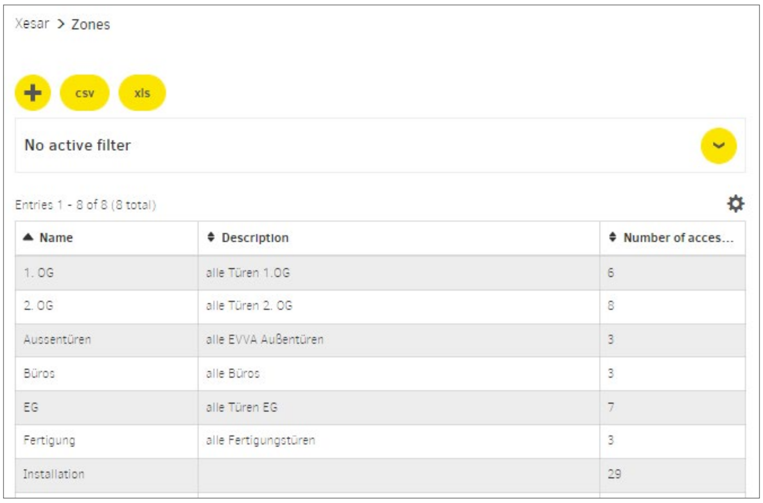
Access points can be merged into areas. This is useful if several access points have the same characteristics, e. g. the same authorisations, organisational affiliation, such as departments or building sections.

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.



Xesar > Zones

No active filter

Entries 1 - 8 of 8 (8 total)

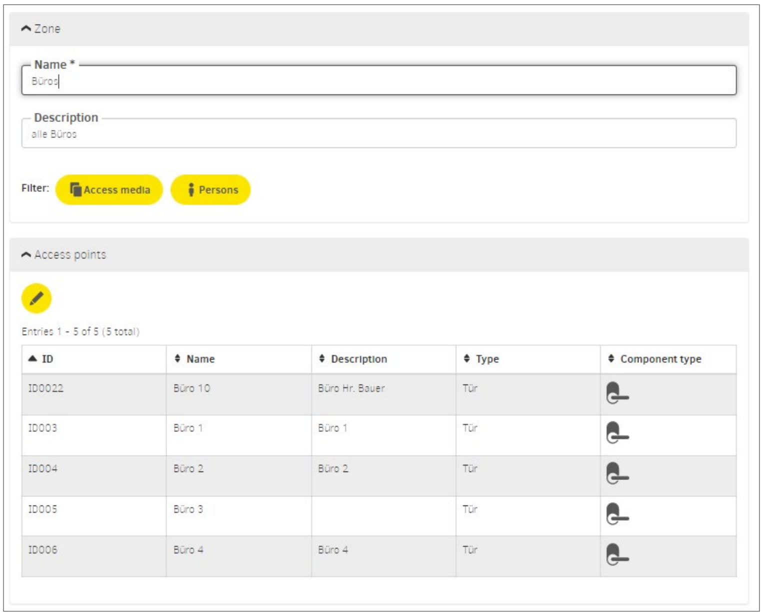
Name	Description	Number of acces...
1. OG	alle Türen 1.OG	6
2. OG	alle Türen 2. OG	8
Aussentüren	alle EVVA Außentüren	3
Büros	alle Büros	3
EG	alle Türen EG	7
Fertigung	alle Fertigungstüren	3
Installation		29

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



Zone

Name *
Büros

Description
alle Büros

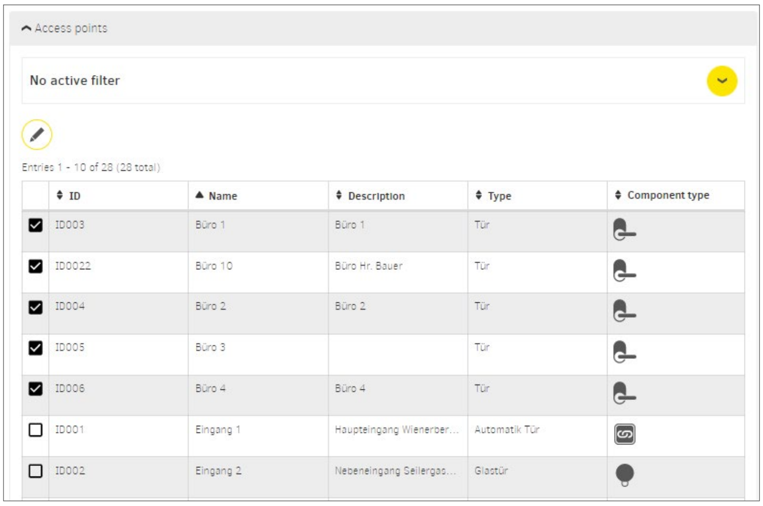
Filter: Access media Persons

Access points

Entries 1 - 5 of 5 (5 total)

ID	Name	Description	Type	Component type
ID0022	Büro 10	Büro Hr. Bauer	Tür	
ID003	Büro 1	Büro 1	Tür	
ID004	Büro 2	Büro 2	Tür	
ID005	Büro 3		Tür	
ID006	Büro 4	Büro 4	Tür	

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



^ Access points

No active filter

Entries 1 - 10 of 28 (28 total)

	ID	Name	Description	Type	Component type
☑	ID003	Büro 1	Büro 1	Tür	
☑	ID0022	Büro 10	Büro Hr. Bauer	Tür	
☑	ID004	Büro 2	Büro 2	Tür	
☑	ID005	Büro 3		Tür	
☑	ID006	Büro 4	Büro 4	Tür	
□	ID001	Eingang 1	Haupteingang Wienerber…	Automatik Tür	
□	ID002	Eingang 2	Nebeneingang Seilergas…	Glastür	

2.9 Authorisation profiles

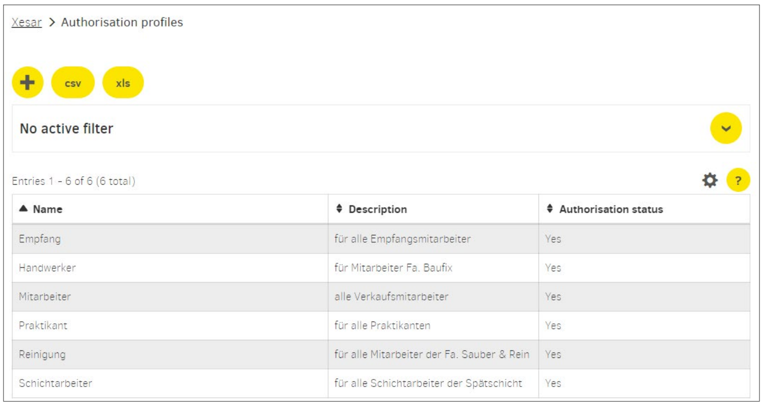
Authorisation profiles describe spatial and temporal access restrictions for access media. These access media can be assigned to persons. This means that a person with an access medium only has access to the access points and areas defined in the authorisation profile and only at the defined times. Access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



No active filter

Entries 1 - 6 of 6 (6 total)

▲ Name	♦ Description	♦ Authorisation status
Empfang	für alle Empfangsmitarbeiter	Yes
Handwerker	für Mitarbeiter Fa. Baufix	Yes
Mitarbeiter	alle Verkaufsmitarbeiter	Yes
Praktikant	für alle Praktikanten	Yes
Reinigung	für alle Mitarbeiter der Fa. Sauber & Rein	Yes
Schichtarbeiter	für alle Schichtarbeiter der Spätschicht	Yes

Authorisation profile:

Mandatory fields are marked with *.

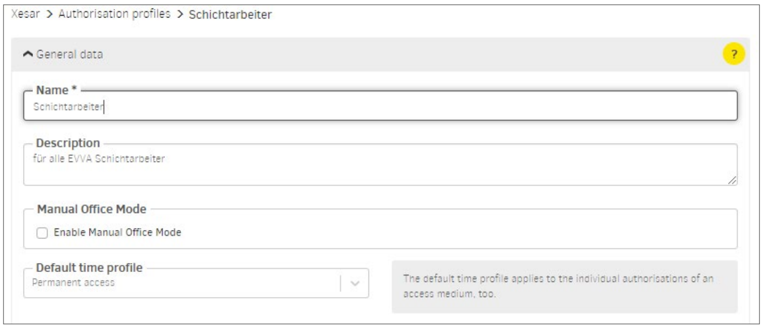
Name:
Name of the authorisation profile, e. g. shift worker

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.



Name *
Schichtarbeiter

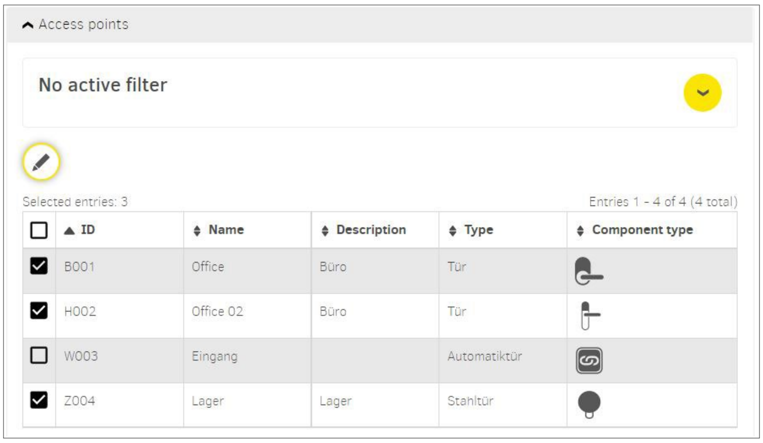
Description
für alle EVVA Schichtarbeiter

Manual Office Mode
□ Enable Manual Office Mode

Default time profile
Permanent access

The default time profile applies to the individual authorisations of an access medium, too.

Selection of installation points:



Access points

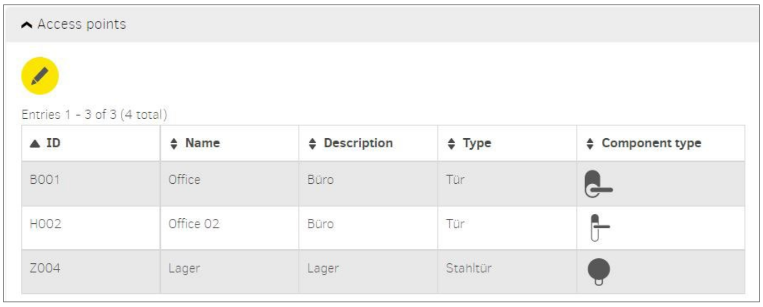
No active filter

Selected entries: 3

Entries 1 - 4 of 4 (4 total)

☐	ID	Name	Description	Type	Component type
☑	B001	Office	Büro	Tür	
☑	H002	Office 02	Büro	Tür	
☐	W003	Eingang		Automatiktür	
☑	Z004	Lager	Lager	Stahltür	

Access to the selected access points:



Access points

Entries 1 - 3 of 3 (4 total)

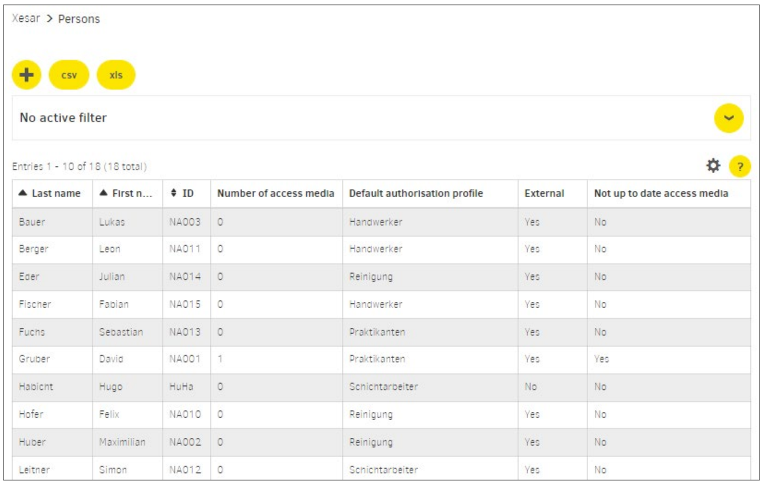
ID	Name	Description	Type	Component type
B001	Office	Büro	Tür	
H002	Office 02	Büro	Tür	
Z004	Lager	Lager	Stahltür	

2.10 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:



No active filter

Entries 1 - 10 of 18 (18 total)

▲ 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

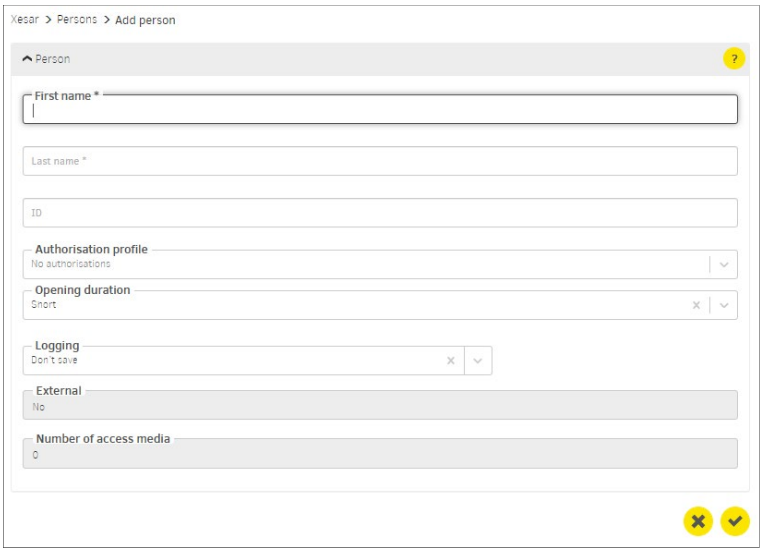
Number of access media:
The number of access media assigned to the person

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.

2.10.1 Adding a person



First name *

Last name *

ID

Authorisation profile
No authorisations

Opening duration
Short

Logging
Don't save

External
No

Number of access media
0

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.

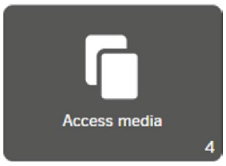
Logging:
Type of event recording - accesses can be recorded indefinitely or for a limited period.

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

2.11 Access media

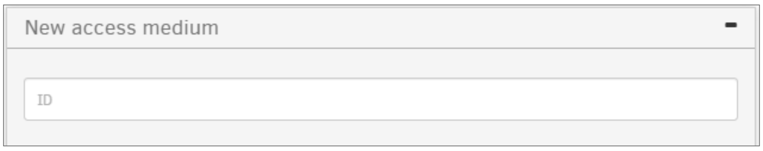


Access media are used to open doors using existing authorisation and to transfer system-specific security data between the access components and the management software via the XVN virtual network (Xesar virtual network).

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.

2.11.1 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)

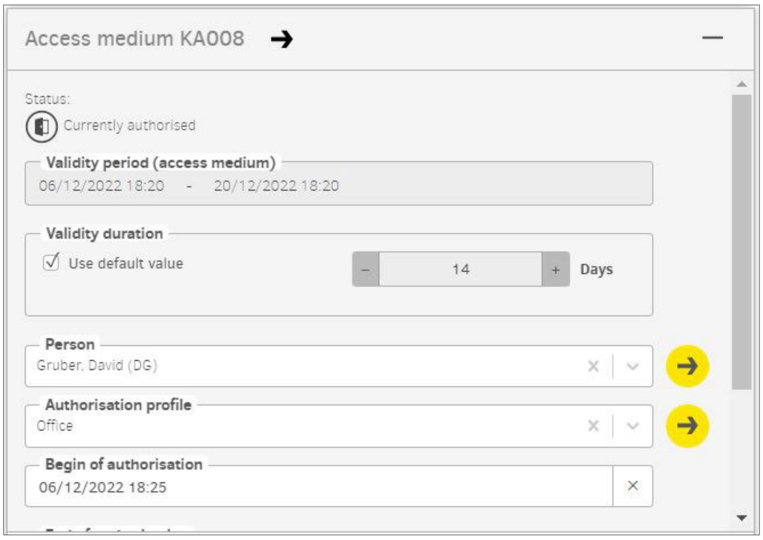
You can assign the access medium an access medium description (e.g. Hans Huber garage, visitor 1 or room 23).

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:



Access medium KA008

Status:
Currently authorised

Validity period (access medium)
06/12/2022 18:20 - 20/12/2022 18:20

Validity duration
☑ Use default value
– 14 + Days

Person
Gruber, David (DG)

Authorisation profile
Office

Begin of authorisation
06/12/2022 18:25

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.

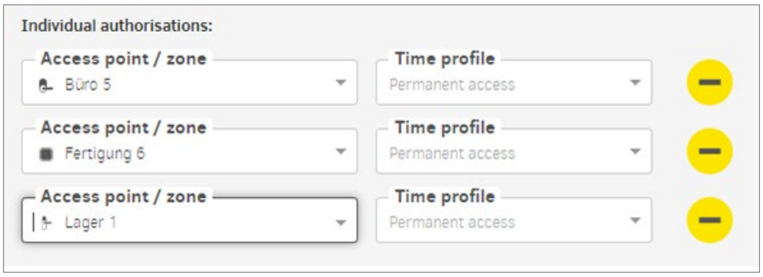
Access medium (substitute access medium) – The field only appears with a new access medium:
In order to create a replacement medium, the access medium to be replaced for the person selected above is selected here with his or her authorisation profile.

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.



Individual authorisations:

Access point / zone	Time profile
Büro 5	Permanent access
Fertigung 6	Permanent access
Lager 1	Permanent access

2.11.2 Add Smartphone as access medium

The following requirements must be met to open a Xesar system with a smartphone:

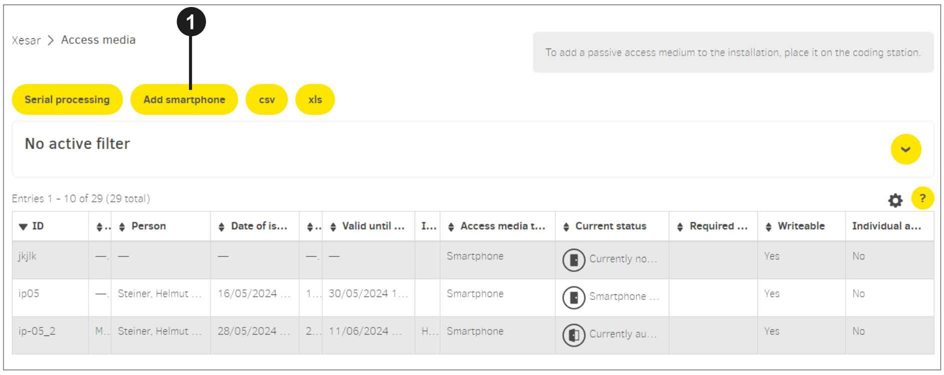
- Xesar software version 3.2 or higher is installed.

- 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.



Xesar > Access media

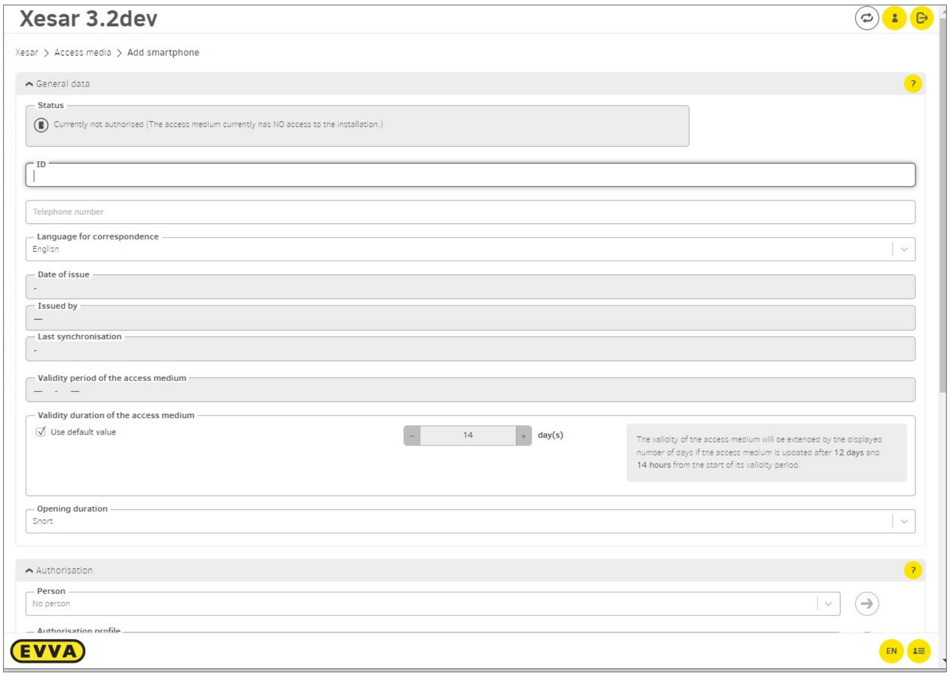
To add a passive access medium to the installation, place it on the coding station.

No active filter

Entries 1 - 10 of 29 (29 total)

▼ ID	♦..	♦ Person	♦ Date of is...	♦..	♦ Valid until ...	I...	♦ Access media t...	♦ Current status	♦ Required ...	♦ Writeable	Individual a...
jkjlk	—.	—	—	—.	—		Smartphone	Currently no...		Yes	No
ip05	—.	Steiner, Helmut ...	16/05/2024 ...	1...	30/05/2024 1...		Smartphone	Smartphone ...		Yes	No
ip-05_2	M..	Steiner, Helmut ...	28/05/2024 ...	2...	11/06/2024 ...	H...	Smartphone	Currently au...		Yes	No

» Press the **Add smartphone** button ❶ to open the details page.



Xesar 3.2dev

Xesar > Access media > Add smartphone

General data

Status: Currently not authorised (The access medium currently has NO access to the installation.)

ID:

Telephone number

Language for correspondence: English

Date of issue: -

Issued by: —

Last synchronisation: -

Validity period of the access medium: — - —

Validity duration of the access medium: ☑ Use default value 14 day(s)

The validity of the access medium will be extended by the displayed number of days if the access medium is updated after **12 days** and **14 hours** from the start of its validity period.

Opening duration: Short

Authorisation

Person: No person

Authorisation profile

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.

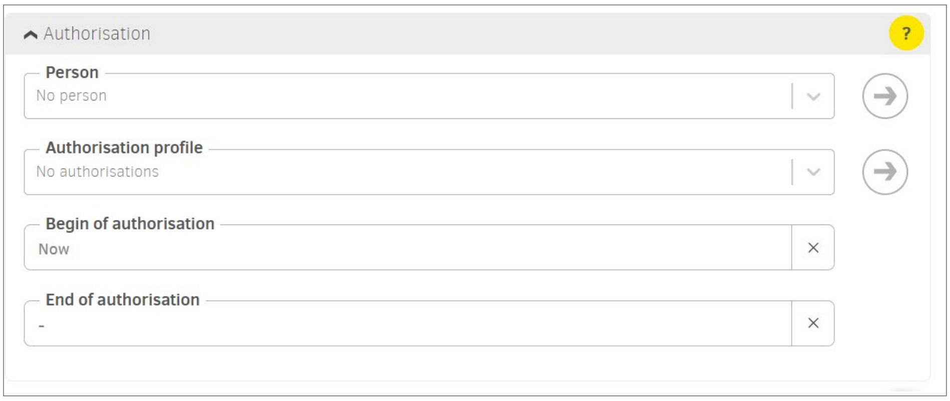
Validity duration:
Information regarding the period for which the access medium is valid.

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:



Authorisation

Person: No person

Authorisation profile: No authorisations

Begin of authorisation: Now

End of authorisation: -

Person:
The access medium can be assigned to a registered person.

Several access media can be assigned to a single person.

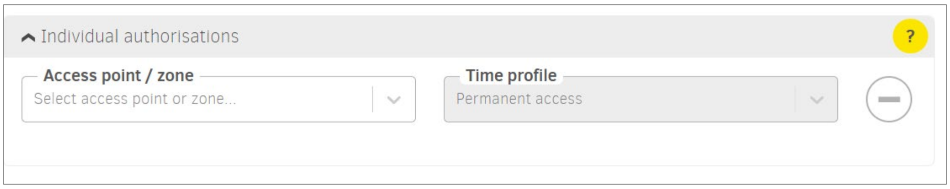
Authorisation profile:
Selection of the desired authorisation profile.

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:



Individual authorisations

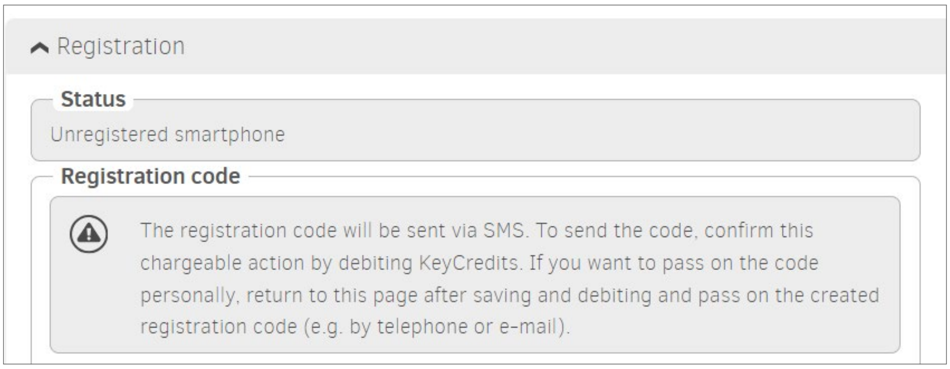
Access point / zone: Select access point or zone...

Time profile: Permanent access

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:



Status

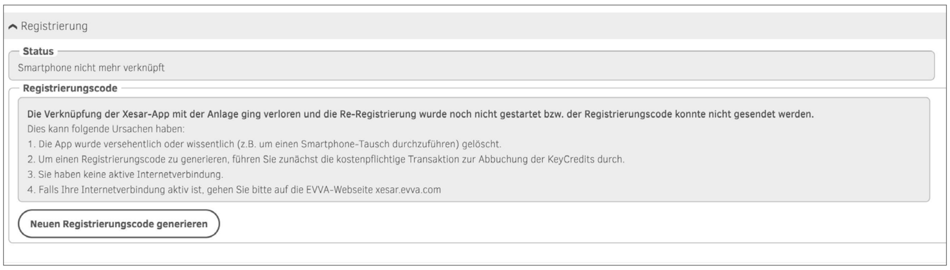
Unregistered smartphone

Registration code

The registration code will be sent via SMS. To send the code, confirm this chargeable action by debiting KeyCredits. If you want to pass on the code personally, return to this page after saving and debiting and pass on the created registration code (e.g. by telephone or e-mail).

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, Key-Credits are required for this promotion (unless a lifetime licence has been purchased).
Make sure that there is enough KeyCredits credit available.



Status

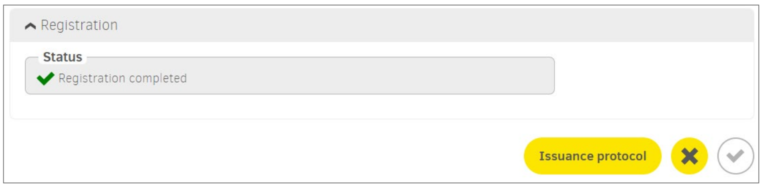
Smartphone nicht mehr verknüpft

Registrierungscode

Die Verknüpfung der Xesar-App mit der Anlage ging verloren und die Re-Registrierung wurde noch nicht gestartet bzw. der Registrierungscode konnte nicht gesendet werden.
Dies kann folgende Ursachen haben:
1. Die App wurde versehentlich oder wissentlich (z.B. um einen Smartphone-Tausch durchzuführen) gelöscht.
2. Um einen Registrierungscode zu generieren, führen Sie zunächst die kostenpflichtige Transaktion zur Abbuchung der KeyCredits durch.
3. Sie haben keine aktive Internetverbindung.
4. Falls Ihre Internetverbindung aktiv ist, gehen Sie bitte auf die EVVA-Webseite xesar.evva.com

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.

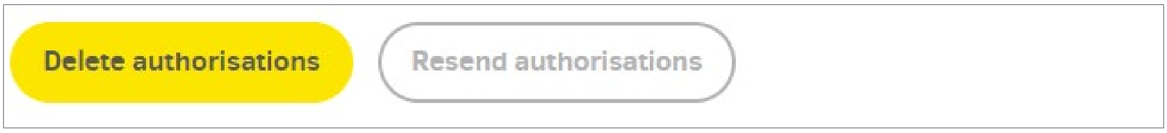


Status

✓ Registration completed

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.



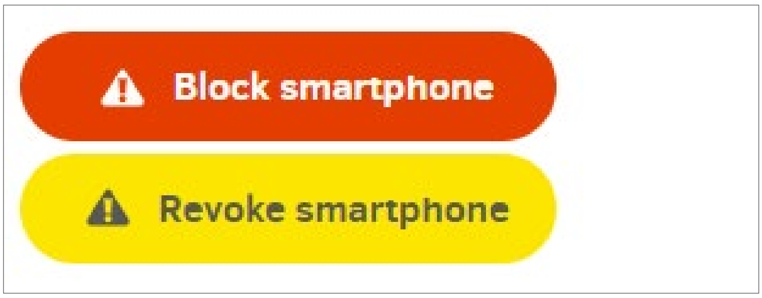
Deleting smartphone authorisations

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.

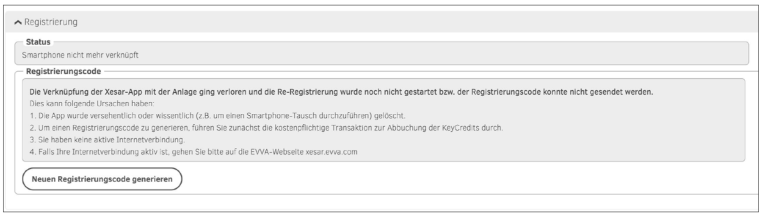
> If the smartphone is withdrawn or authorisations are cancelled, authorisations are only deleted after the transfer has taken place. This is not guaranteed if the smartphone is not physically present.
> If the smartphone is offline or unreachable, it cannot be ensured that the authorisations have actually 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.



Status

Smartphone nicht mehr verknüpft

Registrierungscode

Die Verknüpfung der Xesar-App mit der Anlage ging verloren und die Re-Registrierung wurde noch nicht gestartet bzw. der Registrierungscode konnte nicht gesendet werden.
Dies kann folgende Ursachen haben:
1. Die App wurde versehentlich oder wissentlich (z.B. um einen Smartphone-Tausch durchzuführen) gelöscht.
2. Um einen Registrierungscode zu generieren, führen Sie zunächst die kostenpflichtige Transaktion zur Abbuchung der KeyCredits durch.
3. Sie haben keine aktive Internetverbindung.
4. Falls Ihre Internetverbindung aktiv ist, gehen Sie bitte auf die EVVA-Webseite xesar.evva.com

- 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”).

2.11.3 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).

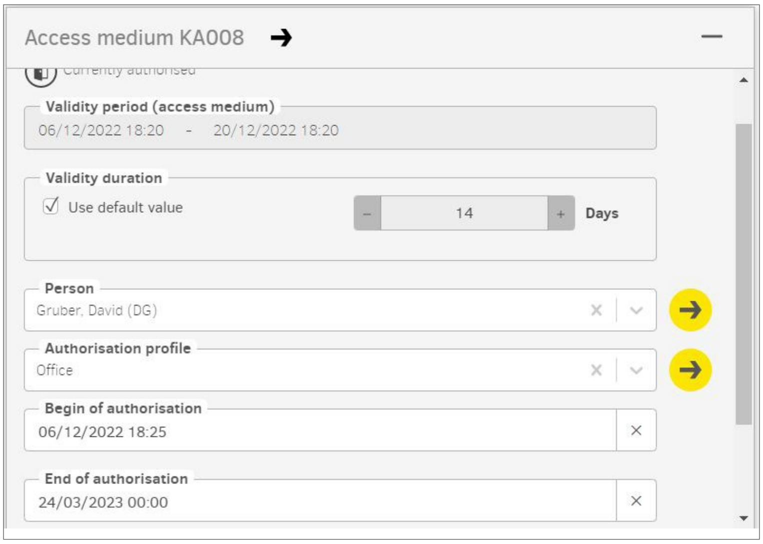
Validity duration:
Information regarding the period for which the access medium is valid.

- **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



Access medium KA008

Currently authorised

Validity period (access medium): 06/12/2022 18:20 - 20/12/2022 18:20

Validity duration: ☑ Use default value – 14 + Days

Person: Gruber, David (DG)

Authorisation profile: Office

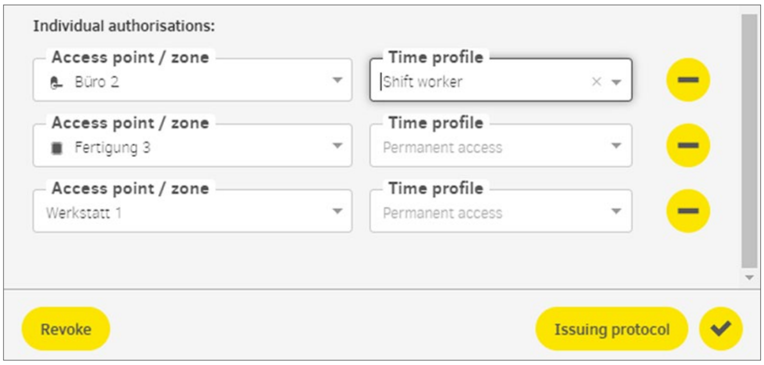
Begin of authorisation: 06/12/2022 18:25

End of authorisation: 24/03/2023 00:00

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.

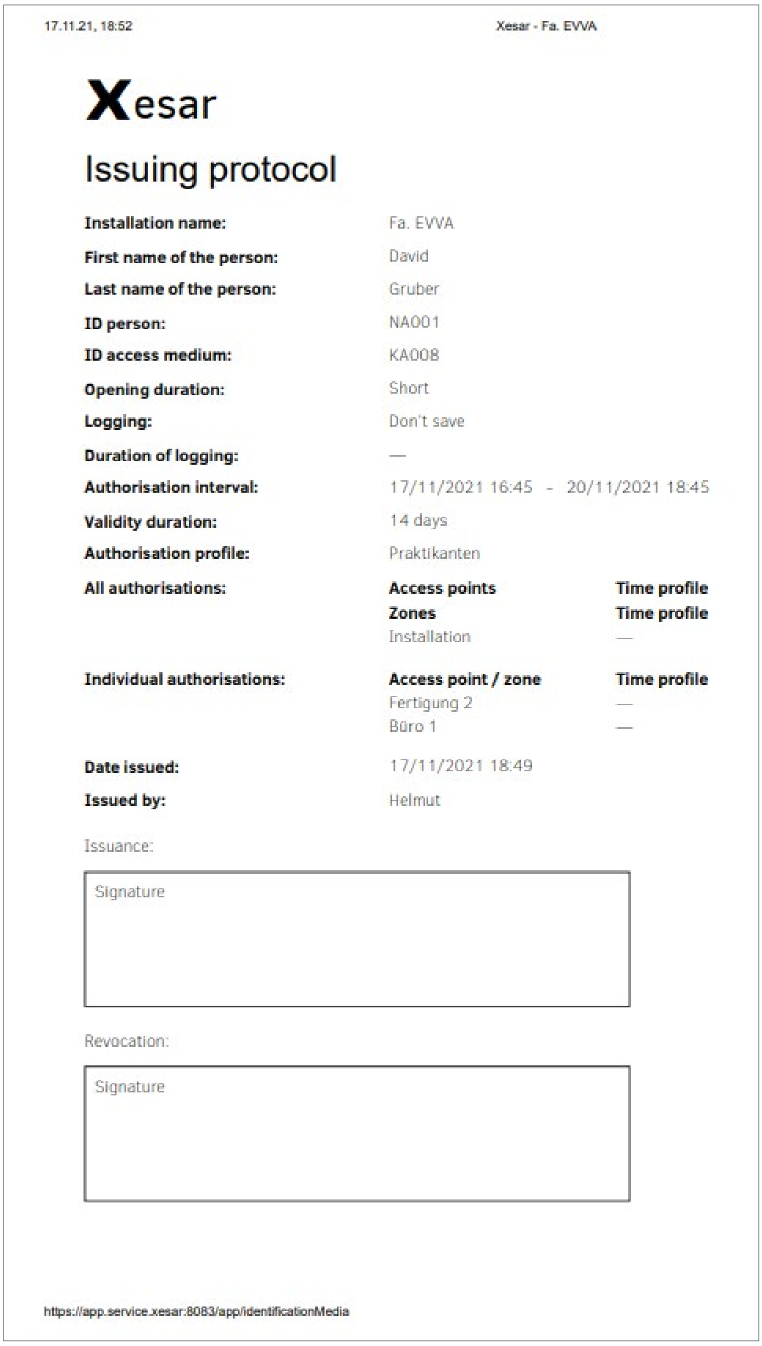


Individual authorisations:

Access point / zone	Time profile
Büro 2	Shift worker
Fertigung 3	Permanent access
Werkstatt 1	Permanent access

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:

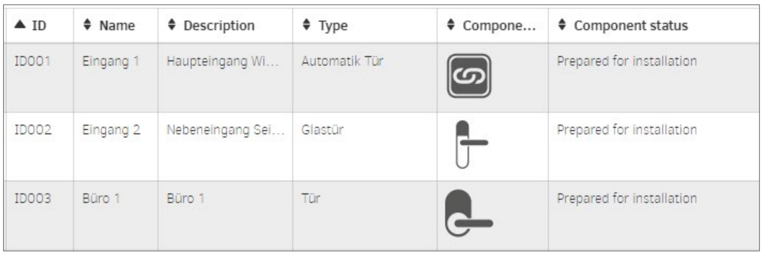
Signature

https://app.service.xesar:8083/app/identificationMedia

2.12 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

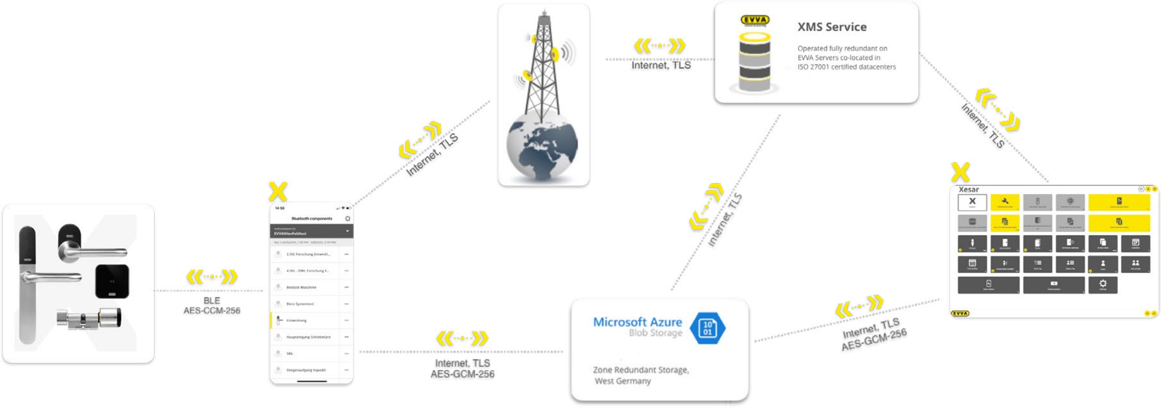
A configuration task is generated in the Xesar software to allow the addition of an access component.

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.

3 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.



4 Xesar app for smartphones

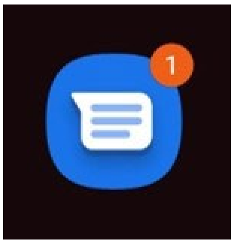
The Xesar app for smartphone with iOS or Android operating systems can be downloaded from the respective app store and installed.

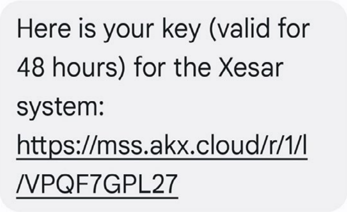
To allow the smartphone to be used as an access medium in a Xesar installation, it must be added to the system and registered. (See chapter "Commissioning the Xesar software", adding a smartphone as an access medium.)

4.1 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.

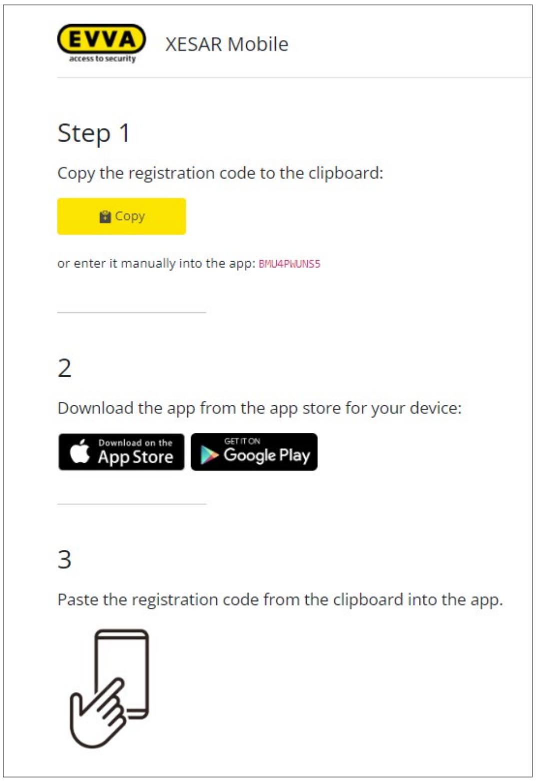




Here is your key (valid for 48 hours) for the Xesar system: https://mss.akx.cloud/r/1/l/VPQF7GPL27

» 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.



XESAR Mobile

Step 1

Copy the registration code to the clipboard:

or enter it manually into the app: BMU4PWUNS5

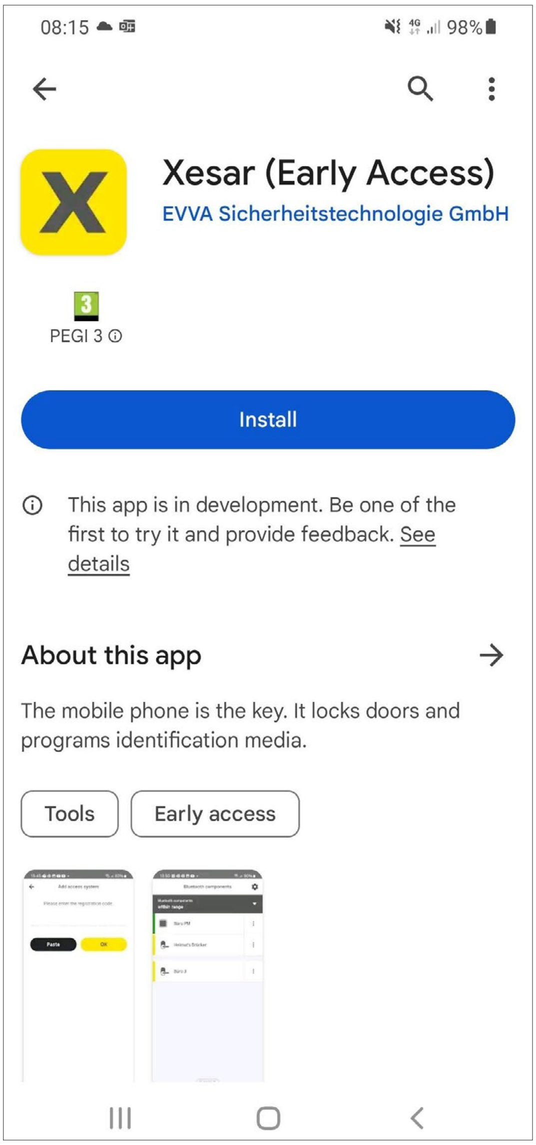
2

Download the app from the app store for your device:

3

Paste the registration code from the clipboard into the app.

- Download and open the Xesar app from the app store.



08:15 98%

Xesar (Early Access)

EVVA Sicherheitstechnologie GmbH

PEGI 3

Install

This app is in development. Be one of the first to try it and provide feedback. See details

About this app

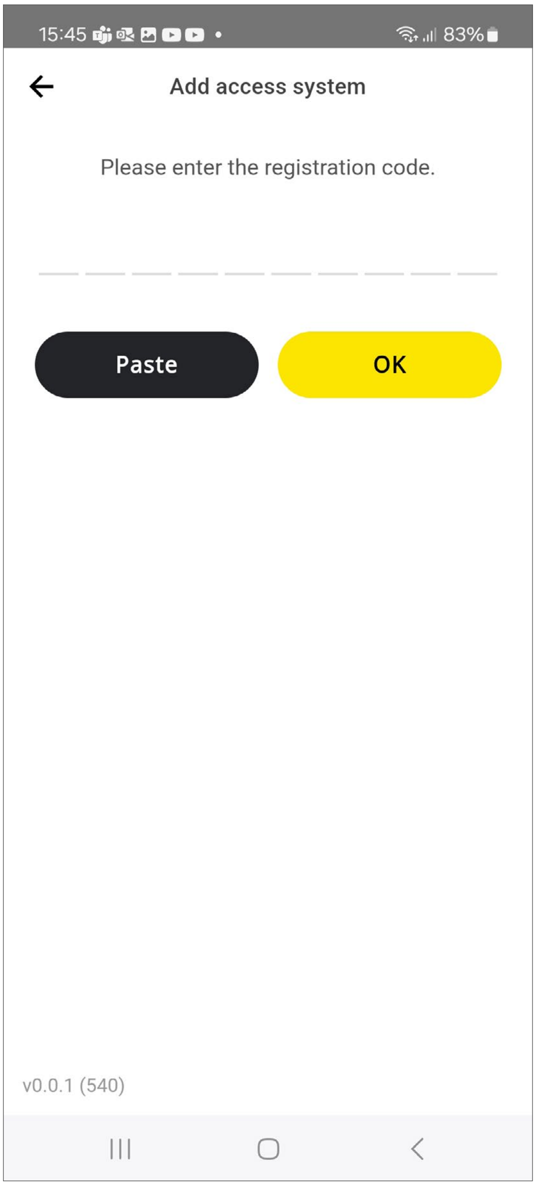
The mobile phone is the key. It locks doors and programs identification media.

Tools

Early access

- Confirm the licence conditions and app authorisations.

» Add the registration code to the installation.

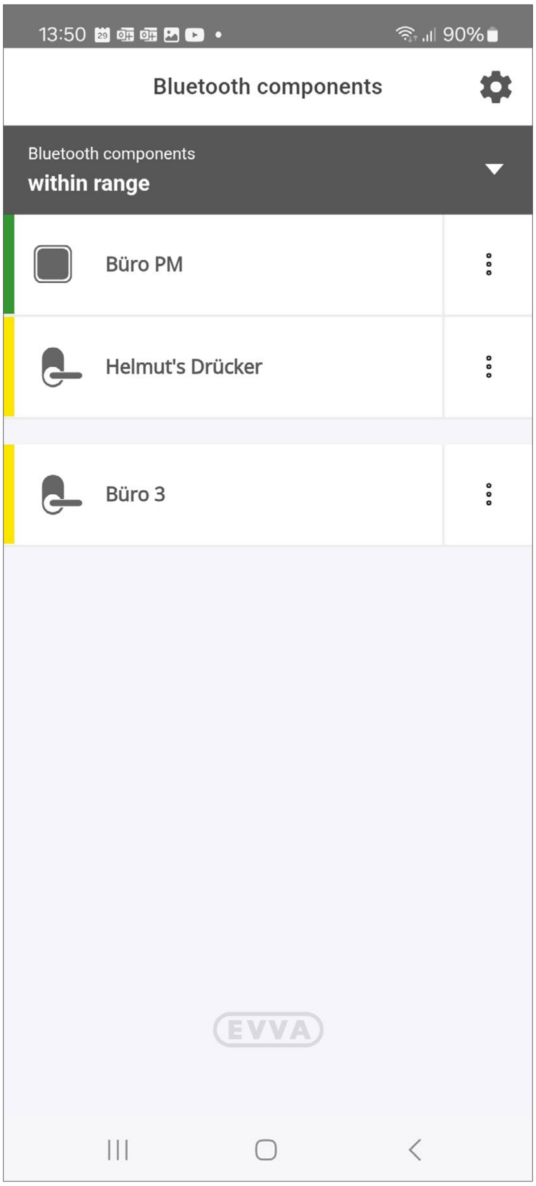


Add access system

Please enter the registration code.

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.



13:50 90%

Bluetooth components

Bluetooth components

within range

Büro PM

Helmut's Drücker

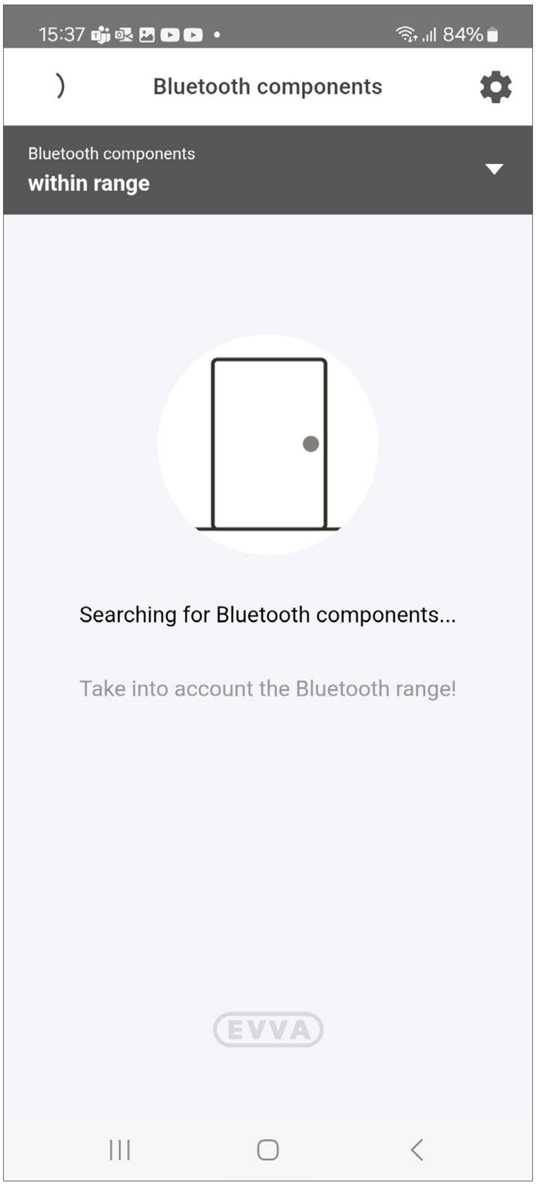
Büro 3

4.2 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.



15:37 84%

Bluetooth components

Bluetooth components
within range

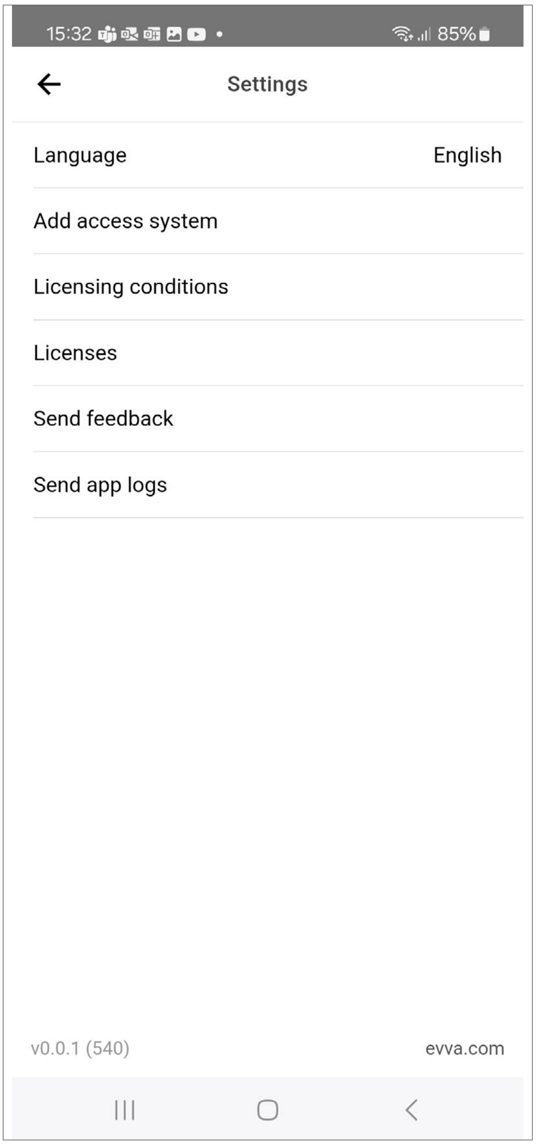
Searching for Bluetooth components...

Take into account the Bluetooth range!

4.3 Xesar app settings

» Click on the gear icon to open the settings page.

The following settings are available:



15:32 • 85%

Settings

Language English

Add access system

Licensing conditions

Licenses

Send feedback

Send app logs

v0.0.1 (540) evva.com

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.

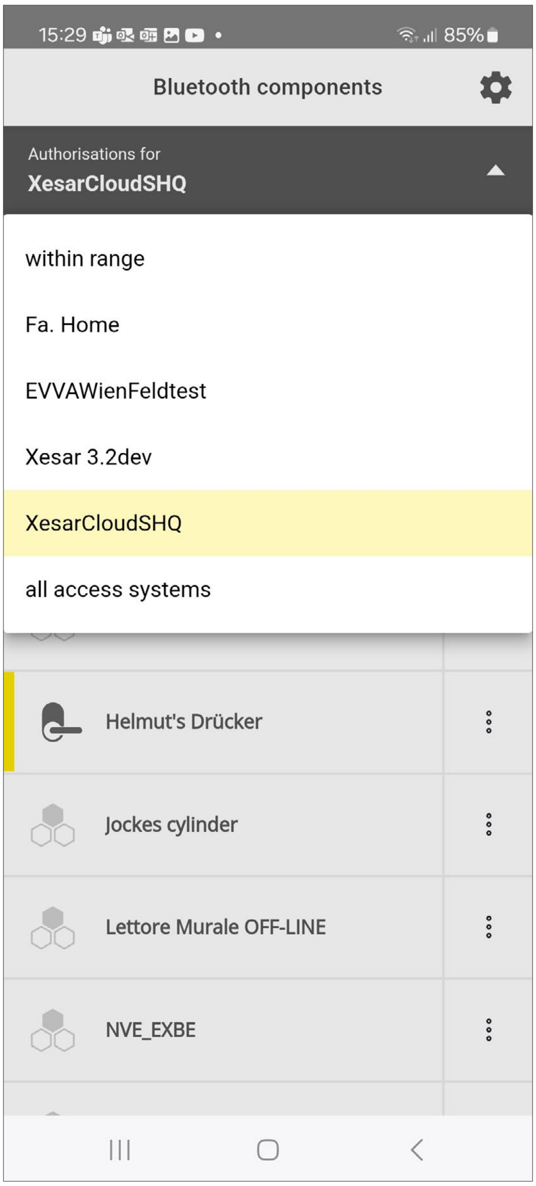
Send feedback:
Email link for sending feedback about the Xesar app to EVVA.

Send app logs:
Send app logs to EVVA if service is requi-red.

4.4 Display of authorised Bluetooth components

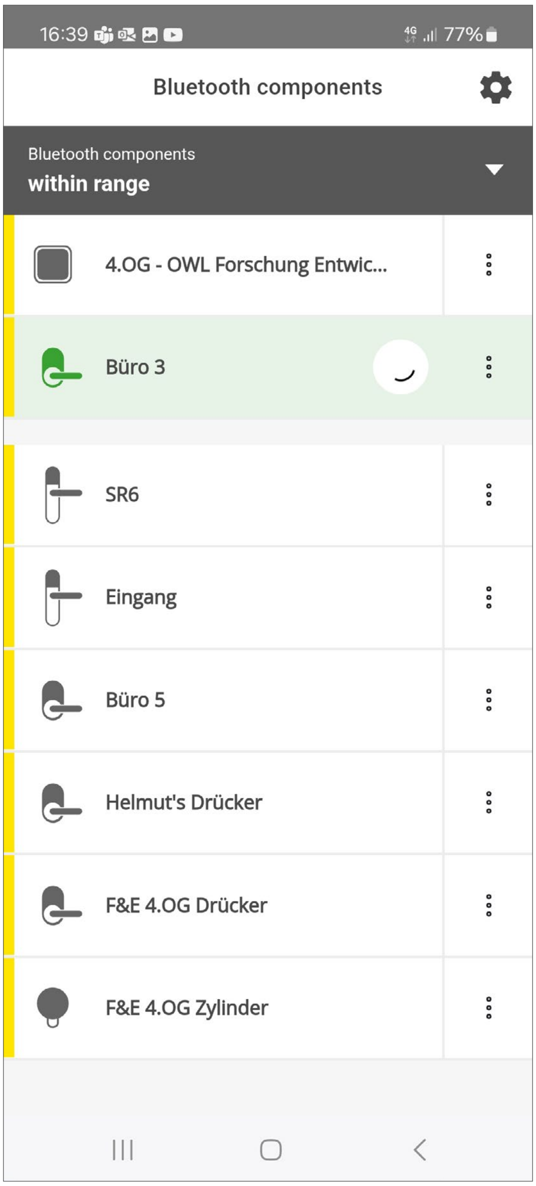
» Click on the down arrow to configure the display of authorised components.

- 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.



16:39 77%

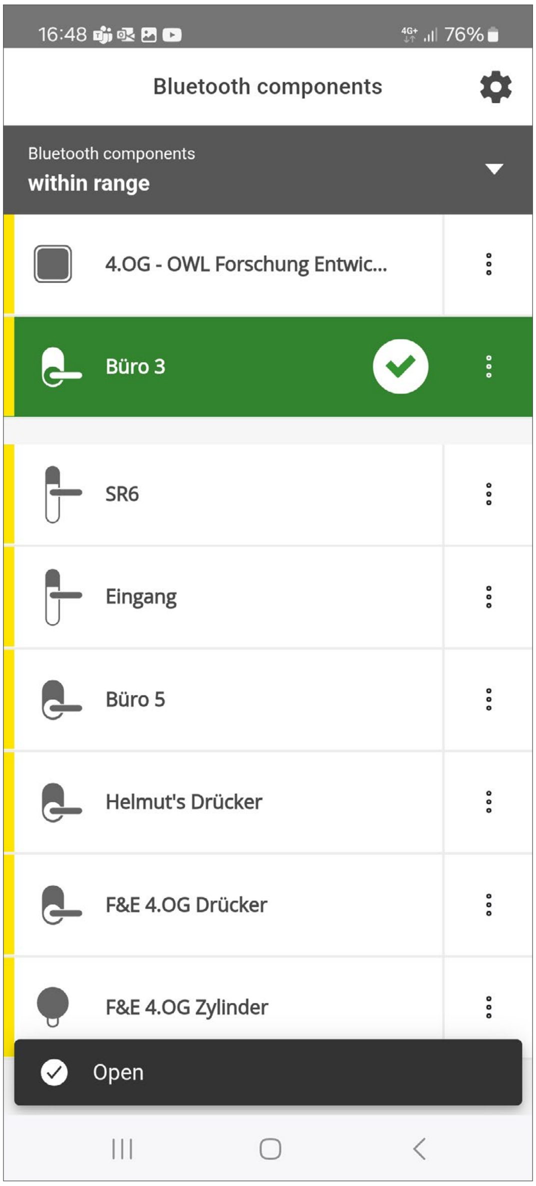
Bluetooth components

Bluetooth components
within range

- 4.OG - OWL Forschung Entwic...
- Büro 3
- SR6
- Eingang
- Büro 5
- Helmut's Drücker
- F&E 4.OG Drücker
- F&E 4.OG Zylinder

Depending on the BLE connection, opening may take a few seconds.

Successful opening is confirmed on the screen.



16:48 76%

Bluetooth components

Bluetooth components

within range

4.OG - OWL Forschung Entwic...

Büro 3 ✓

SR6

Eingang

Büro 5

Helmut's Drücker

F&E 4.OG Drücker

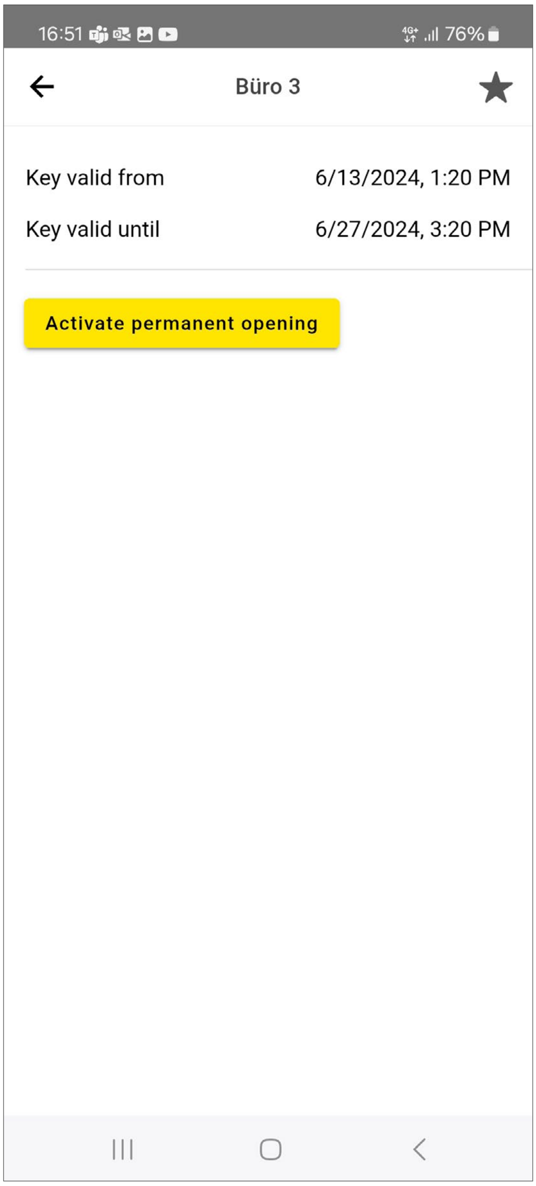
F&E 4.OG Zylinder

✓ Open

4.5 Activating and deactivating manual permanent opening (manual office mode)

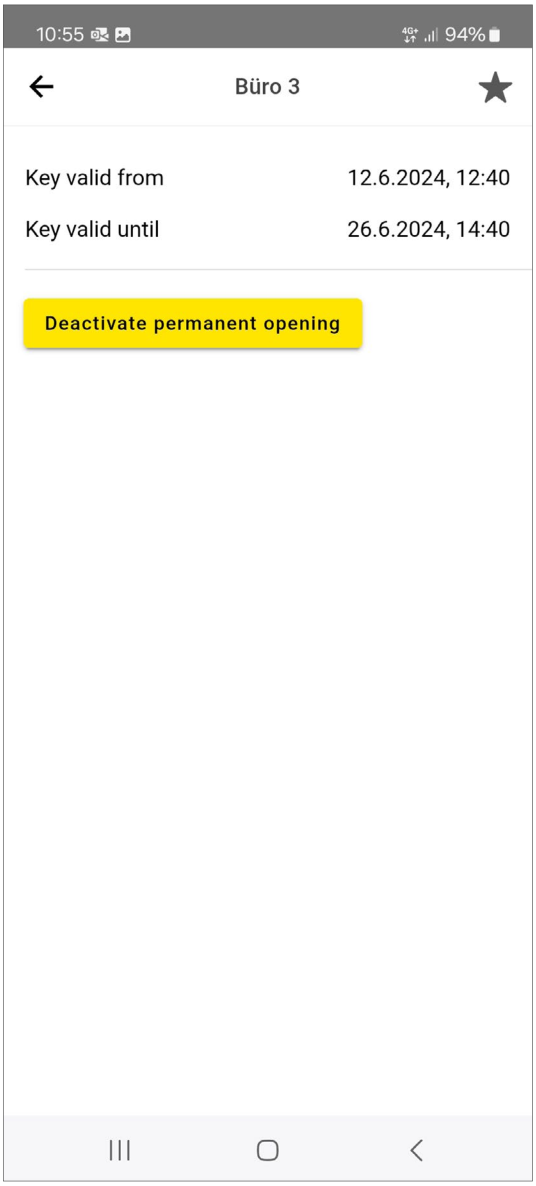
» To access the manual permanent access point function, please click on the 3-point icon located next to the access point location to open the submenu.

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.



Key valid from 6/13/2024, 1:20 PM

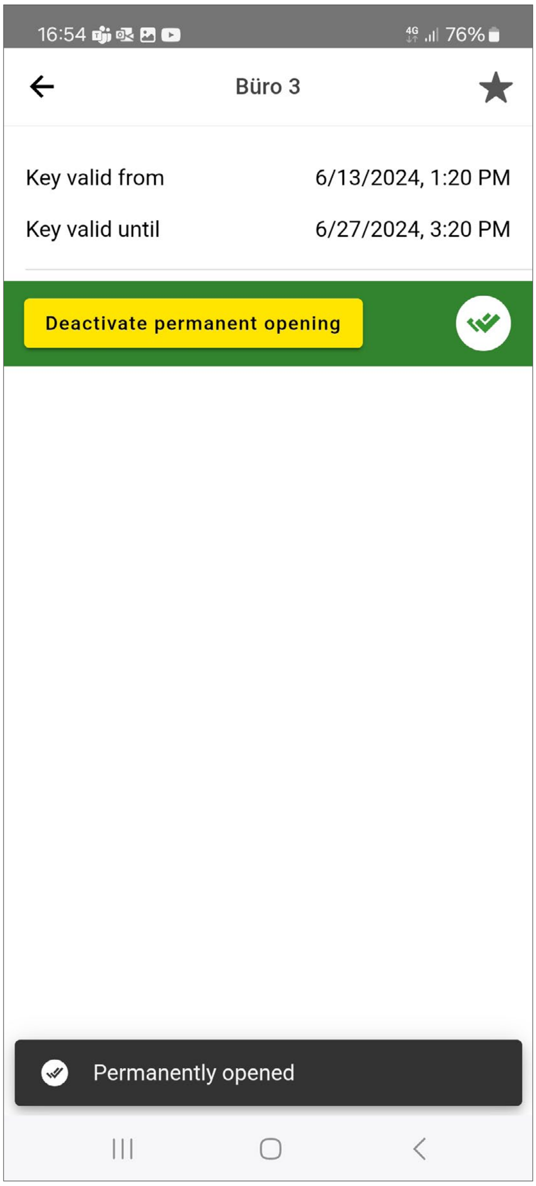
Key valid until 6/27/2024, 3:20 PM



Key valid from 12.6.2024, 12:40

Key valid until 26.6.2024, 14:40

» 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.



16:54 76%

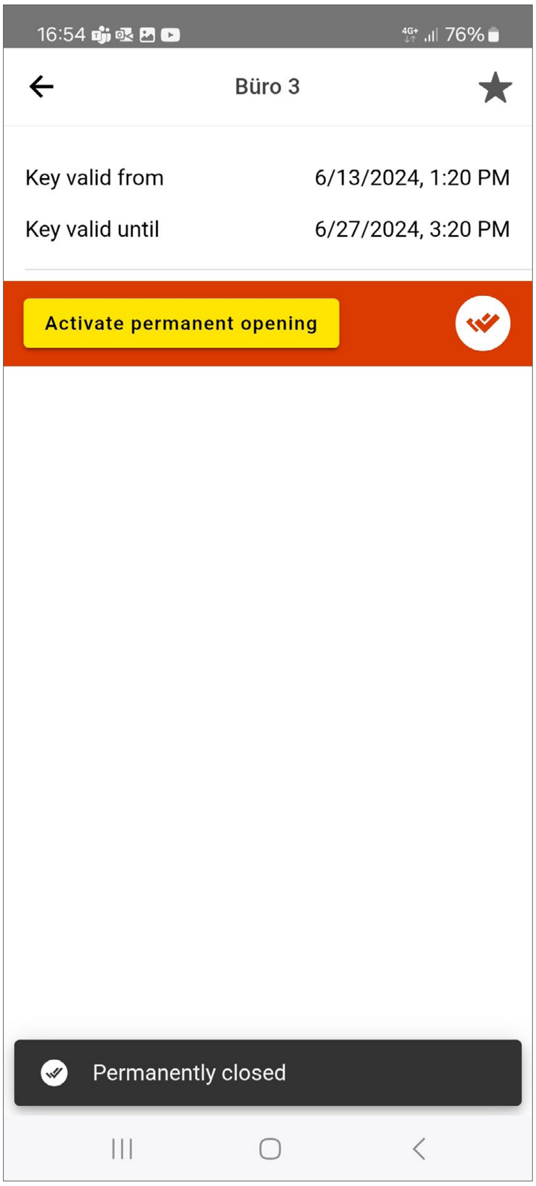
Büro 3

Key valid from 6/13/2024, 1:20 PM

Key valid until 6/27/2024, 3:20 PM

Deactivate permanent opening

Permanently opened



16:54 76%

Büro 3

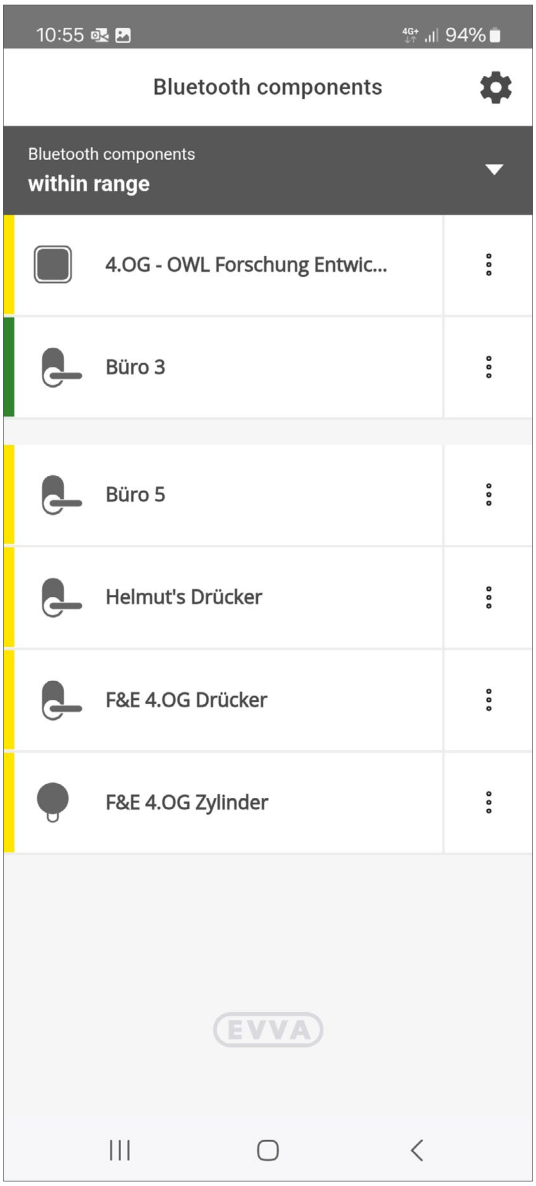
Key valid from 6/13/2024, 1:20 PM

Key valid until 6/27/2024, 3:20 PM

Activate permanent opening

Permanently closed

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.



10:55 94%

Bluetooth components

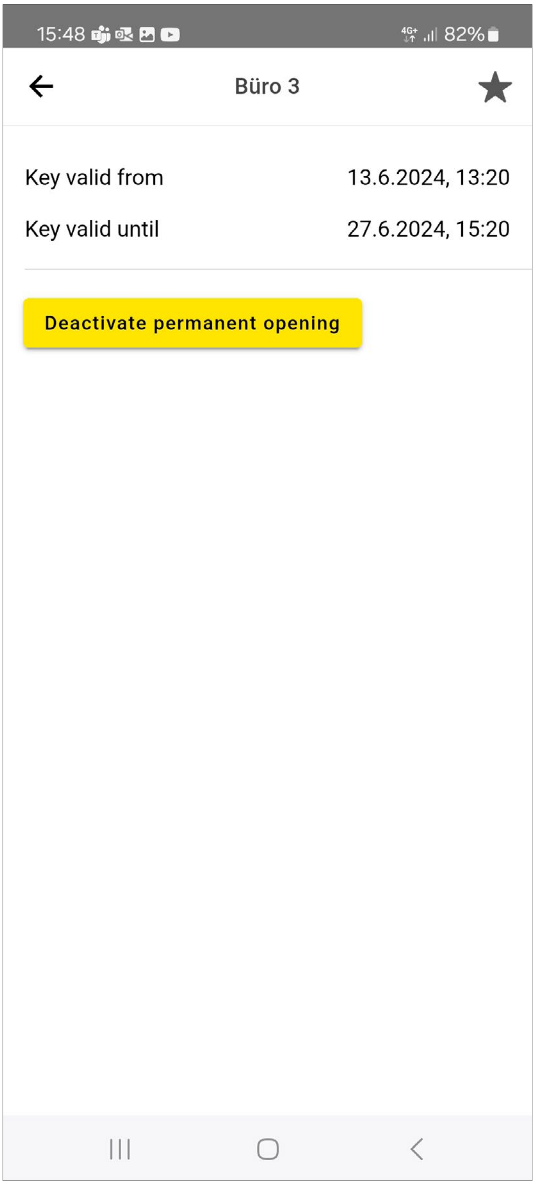
Bluetooth components
within range

- 4.OG - OWL Forschung Entwic...
- Büro 3
- Büro 5
- Helmut's Drücker
- F&E 4.OG Drücker
- F&E 4.OG Zylinder

4.6 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.

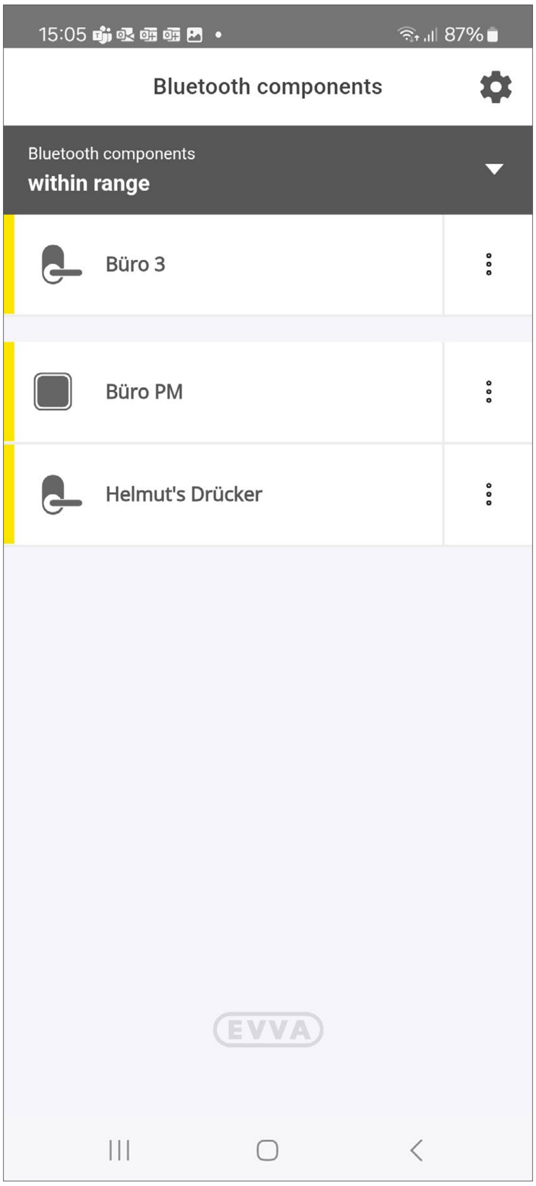
❗ Several installation access points can also be marked as favourites.



15:48 82%

Büro 3

Key valid from	13.6.2024, 13:20
Key valid until	27.6.2024, 15:20



15:05 87%

Bluetooth components

Bluetooth components
within range

- Büro 3
- Büro PM
- Helmut's Drücker

www.evva.com