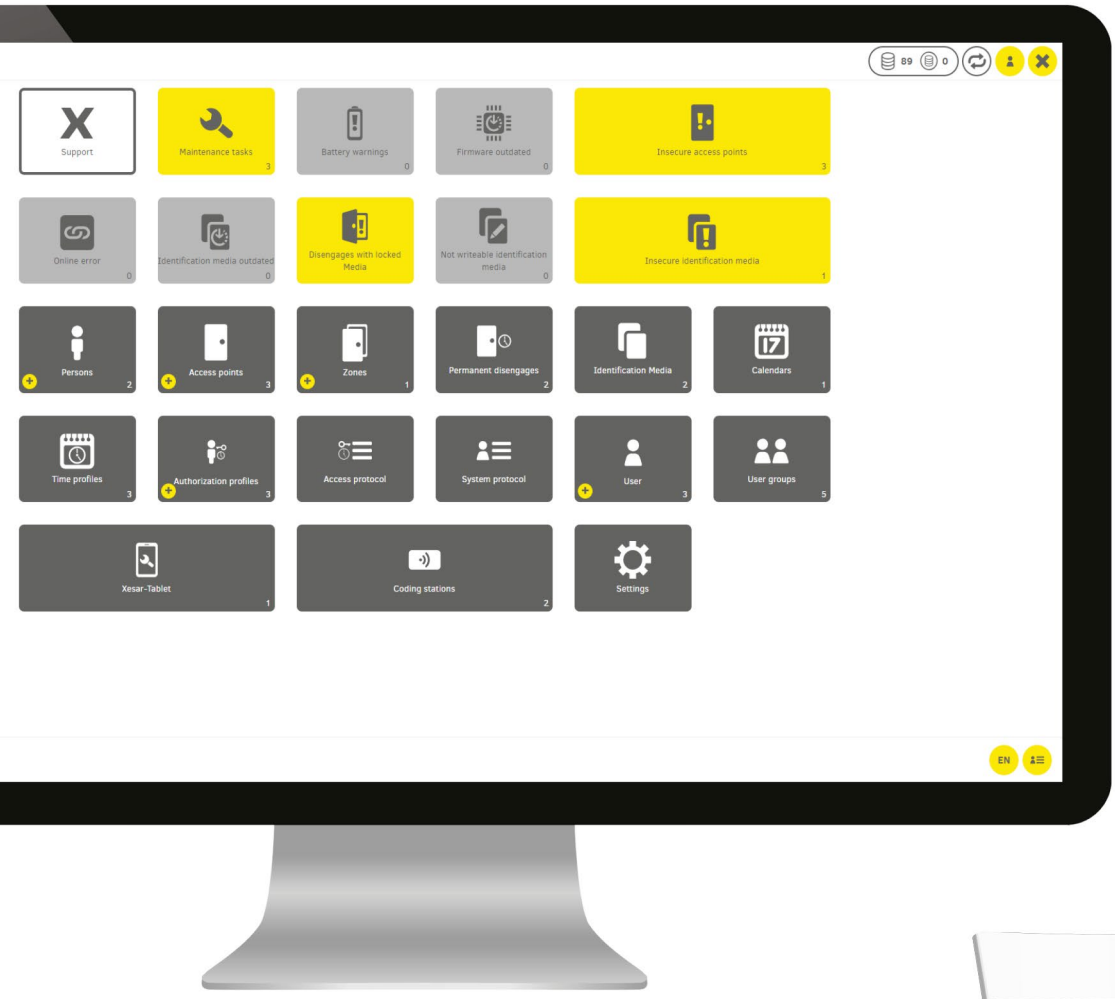


Xesar

Commissioning Xesar software

Imprint

Product code: I.AN.INB.X.R3-1.SEN | 22R1

Version: Xesar 3.1 | 3.1.x
Edition: 02/2022 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/

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

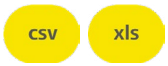
1.4 Explanation of Xesar software symbols

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		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

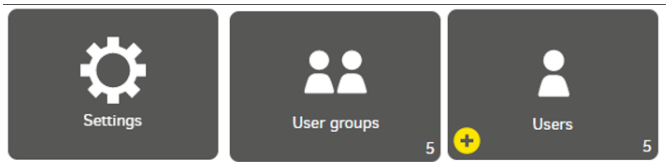
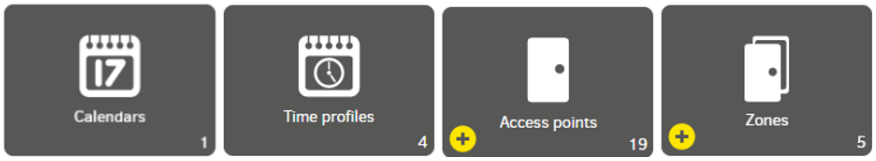
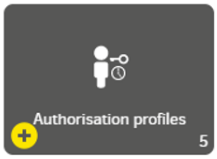
#	Status	Symbol	Explanation
29	Lists export		Export the displayed list as a csv file or as an xls file
30	List view settings		Illustration of list view regarding column selection, number of lines per page, save settings and reset
31	Backup button		A backup of the system data is created in the Installation 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

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.

#	Status	Visualisation	Explanation
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.
9	Deactivated 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

Step 1	
Step 2	
Step 3	
Step 4	

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** symbol. All lists can be exported and printed as .csv or .xlsx files. The original file must use 65001: Unicode (UTF-8).

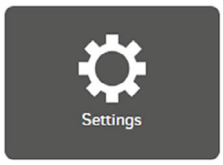
Mandatory fields are marked with *****.

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

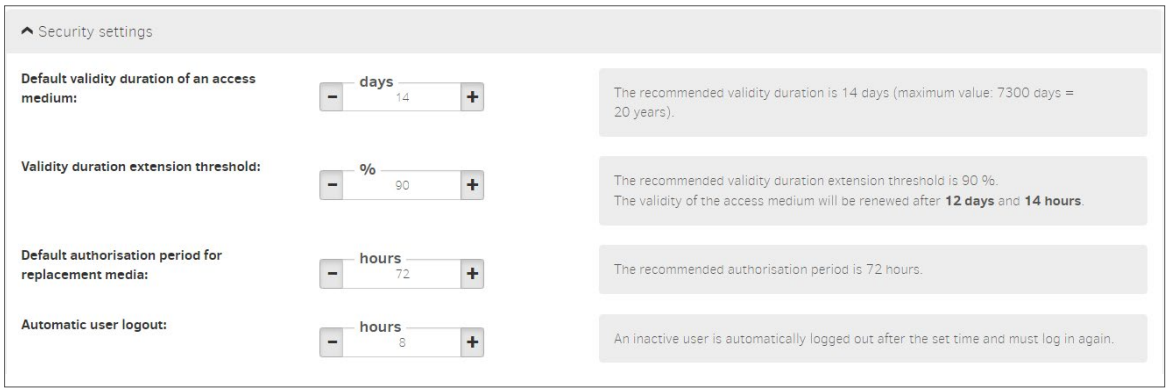
Double-clicking on the column divider adjusts the column width to the column header.

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

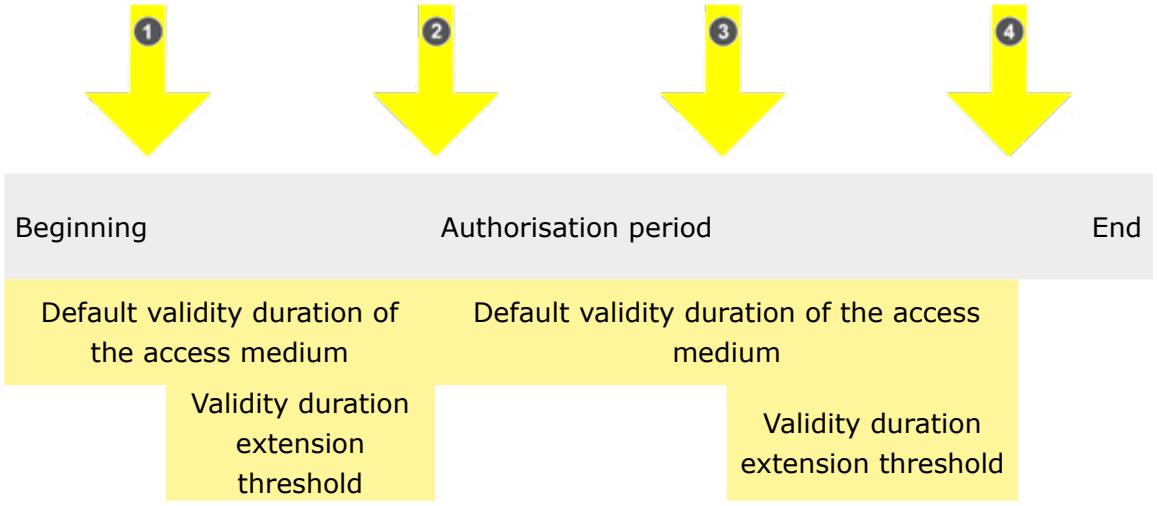
2.2 Settings



2.2.1 Security settings



2.2.2 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 an access medium:

The default validity duration is the preset period of time during which the access medium is valid after updating on the coding station or Xesar online wall reader.

The default validity duration can be individually set when issuing access media.
If the default validity duration has ended, the access medium becomes invalid and may need to be updated on the coding station or the Xesar online wall reader.
The shorter the default validity duration, the more secure the system, as the access medium becomes invalid earlier.

The recommended validity duration is 14 days.

The maximum validity duration is 7300 days (about 20 years).

Extension threshold for the validity duration:

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.

Default authorisation period for replacement media:

The default authorisation period for replacement identification 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

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 online wall readers. 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.

As daily execution time, always select a time when the system is running and the Xesar online wall reader is online (e.g. office times)!

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

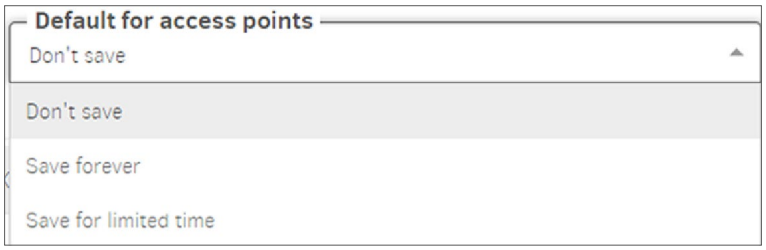
Personal reference settings:

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)

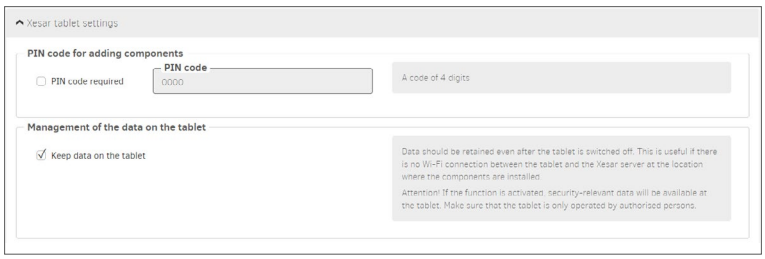


Personal and component-specific settings are defined in the tiles “Persons” or “Access points – Component”.

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.

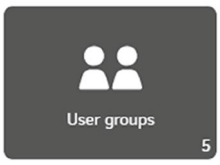
Management of data on the Xesar tablet:
You can activate retention of data on the tablet after switching off the tablet.

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



2.3 User groups

The authorisations for users are defined within the user groups.



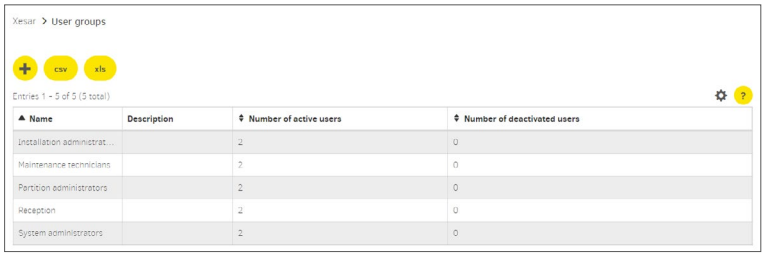
Users manage the system using the Xesar software. Any number of users can be created with various authorisations (depending on their function). These different authorisations are defined in the user groups.

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.



The following predefined user groups are available for selection:

System administrator
is only allowed to modify user passwords

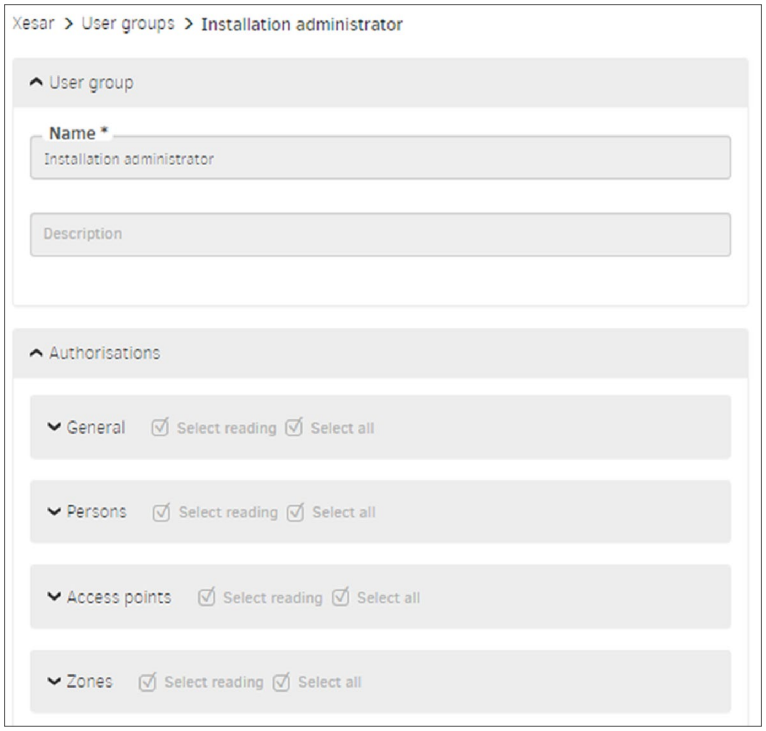
Installation manager
has all authorisations except to change user passwords

Maintenance technician
has limited, maintenance-relevant authorisations

Partition manager
has limited, administration-relevant authorisations

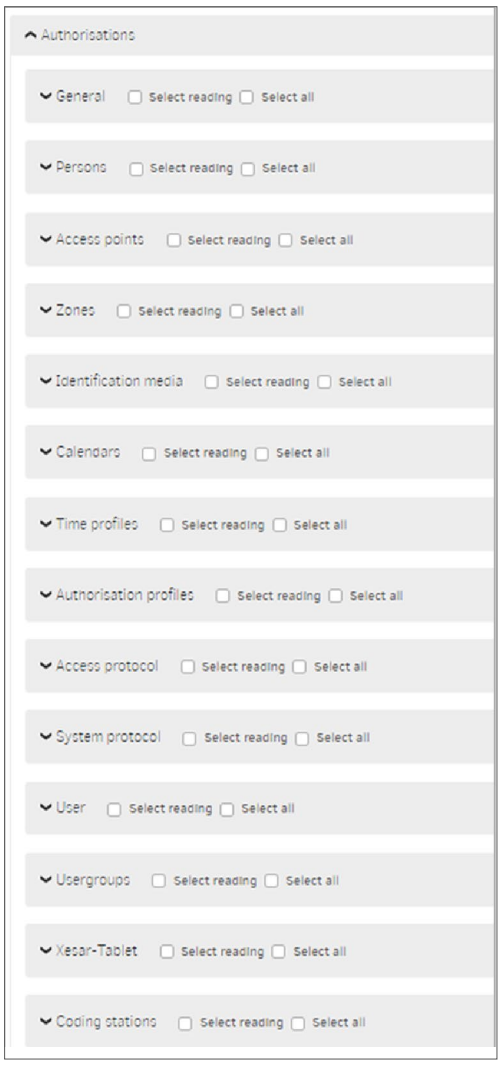
Front desk
has limited, reception-relevant authorisations

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.

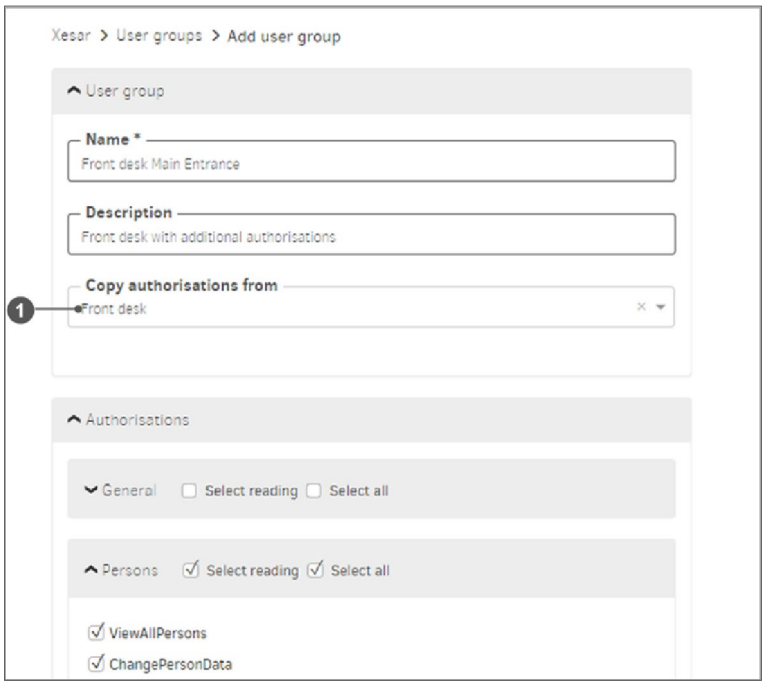


The authorisations are grouped as tiles on the dashboard.

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.

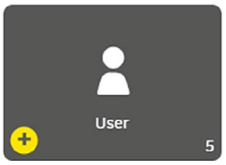
Special authorisation groups can be generated as required. In such cases, please contact the EVVA Technical Office.

Possibility to restrict admission authorisation profile:

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

Example:
The front desk user group may only assign access media with the authorisation profiles employee, trainee, cleaning 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.

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).

Click the "**Add**" symbol to add a new user. The number of registered users is displayed in the User tile.

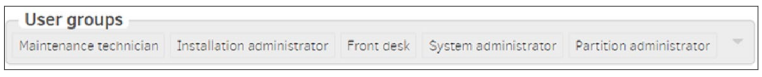
Users are also persons who have access authorisations in the system with access media assigned to them.

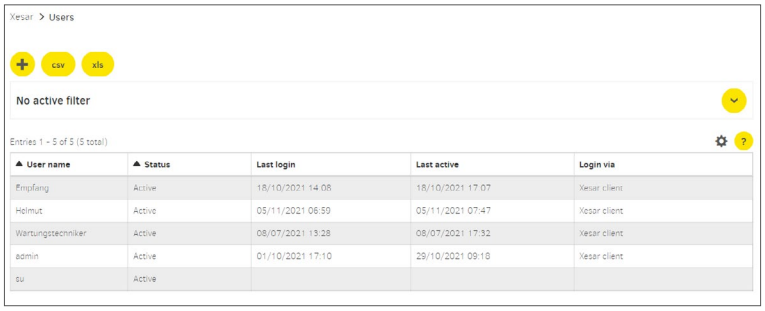
All registered users are displayed in the user overview list.

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

- **su**
  As system administrator, is only 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
with additional information about the new user

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

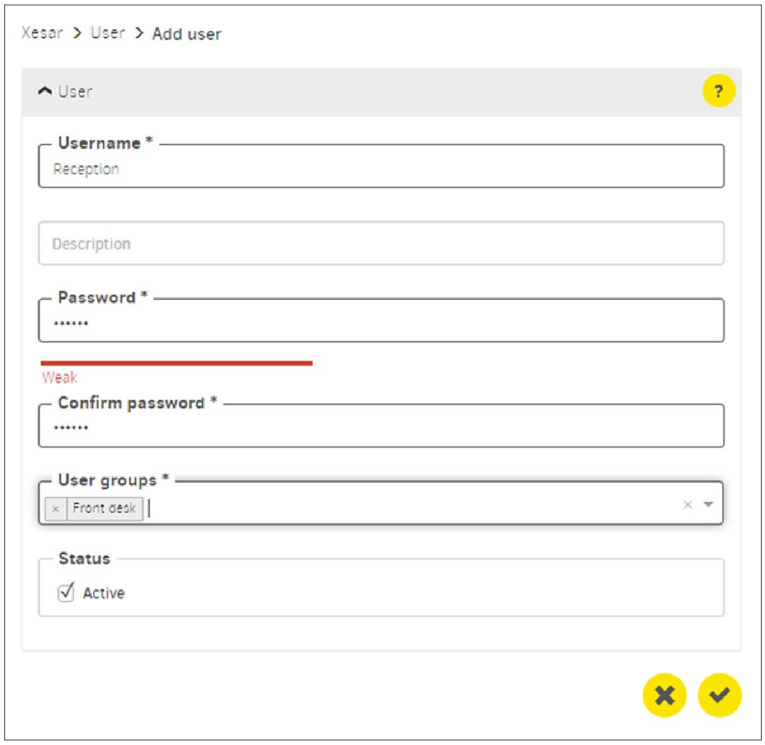
Re-enter password
Re-enter the selected password.

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.



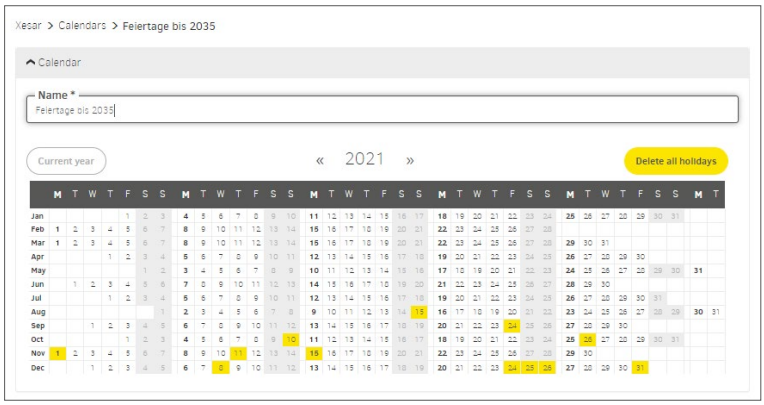
Download configuration
The respective user certificate (configuration) is downloaded. The user certificate is required for secure third-party system interface actions (e.g. personal data import via the third-party system interface).

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.



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.

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. You set the manual office mode in the respective menu item under **Access point** and **Authorisation profiles**.

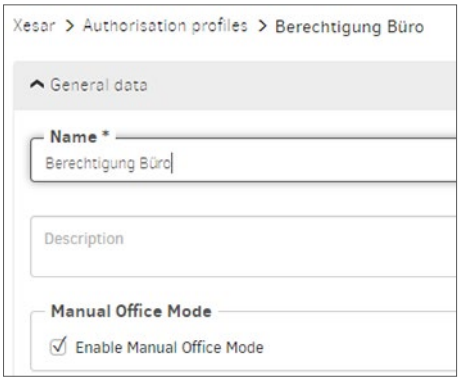
Manual office mode is activated by holding an authorised access medium to the Xesar access component twice. You will be notified by a corresponding optical and acoustic confirmation (see chapter “Event signalling”).

The manual office mode is automatically terminated at the defined closing time or manually terminated by again holding an authorised access medium to the Xesar access component twice. You will be notified by a corresponding optical and acoustic confirmation (see chapter “Event signalling”).

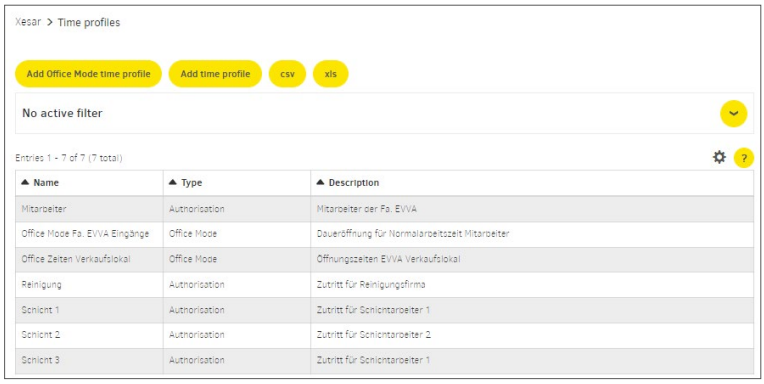
Activate manual office mode and shop mode:

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

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



Time profiles view:



2.6.1 Add office mode time profile

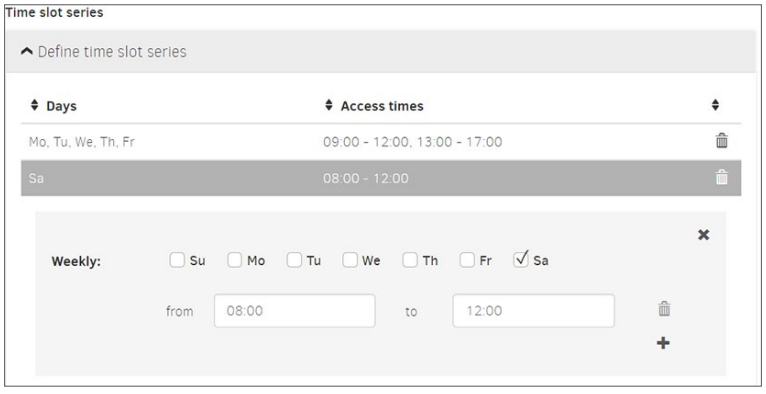
The “permanent opening” function is available for Xesar access components.

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.

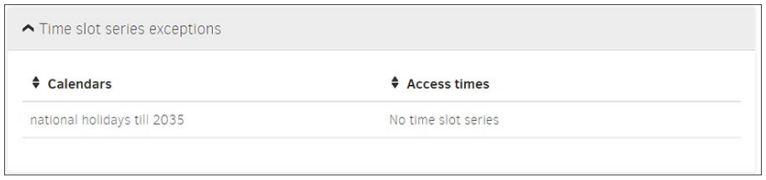
In total, a maximum of 5 different time slots or times per weekday or calendar can be added.

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.



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.



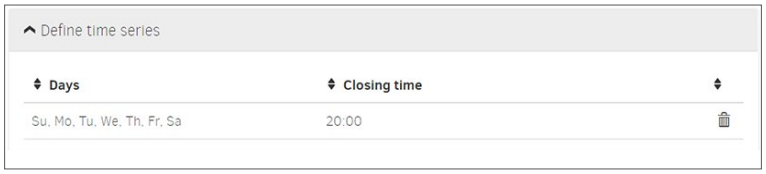
Time series:

Time series define times at which the manual office mode (manual permanent release) automatically ends. 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.

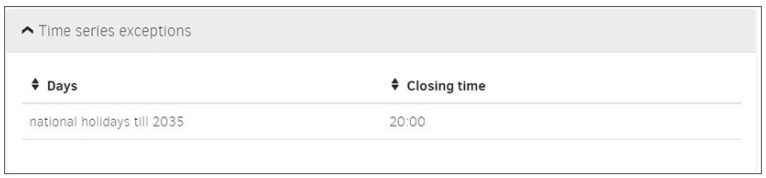
A maximum of 35 time series are possible.

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



Exception to the time series:

The closing time can be changed for holidays.



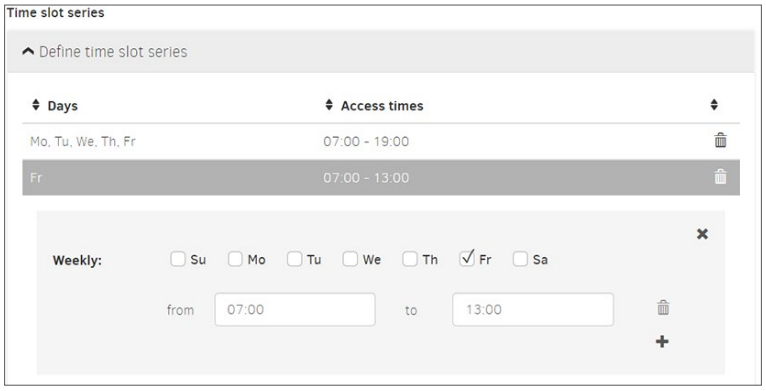
2.6.2 Adding a time profile

Time profiles can be added for persons and access media.

You can create a maximum of 24 time slot series.

Limits to authorisations:

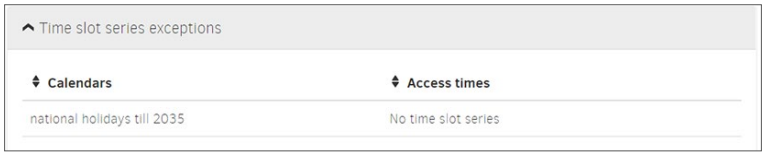
Example, access times for employees:
Monday to Friday from 7:00 am to 7:00 pm and Saturday from 7:00 am to 1:00 pm.



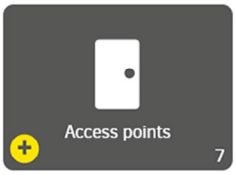
Time slot series exceptions:

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.



2.7 Access 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:
free 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

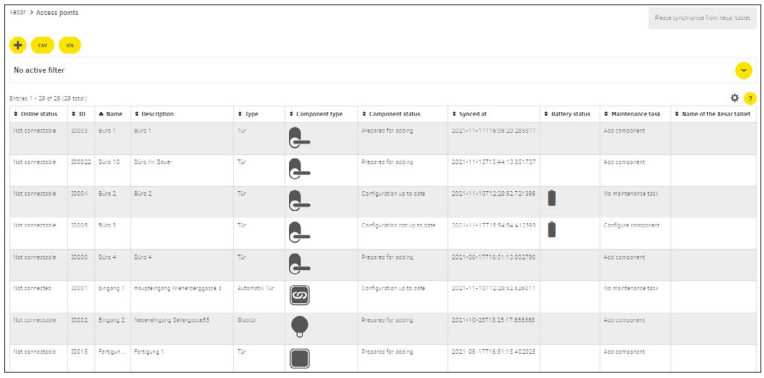
Component status:
describes the current status of the component, e.g. prepared for adding

Synced at:
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 of the access point, e.g. configure, remove, add components, firmware update

Name of the Xesar tablet:
Name of the tablet with the synchronised open maintenance task of the access point



2.7.1 Add access point

Select the desired access component.

2.7.2 Describe access point

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

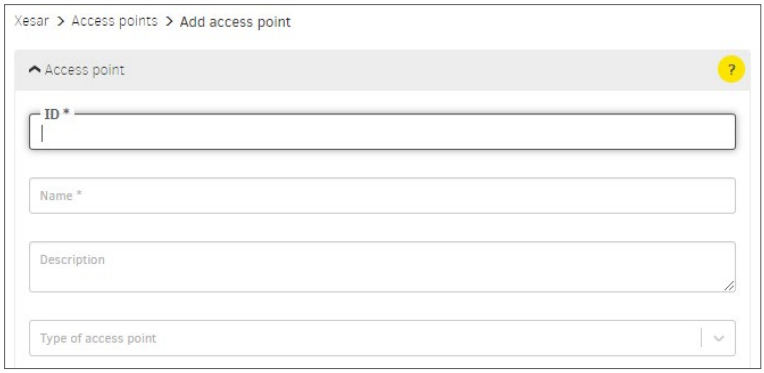
Mandatory fields are marked with *.

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

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

Description:
free 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 time for which the access component grants access, after authorisation, 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 the person is authorised at the Xesar access component.

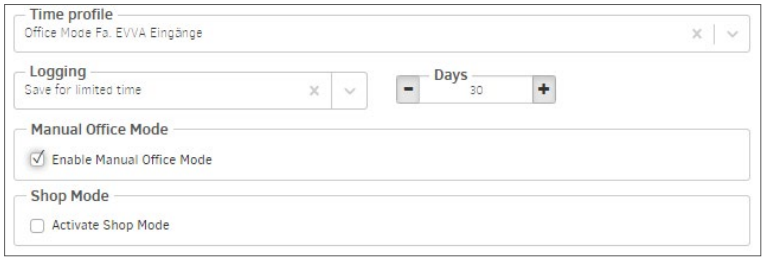
The assignment of the opening duration to the person or the access medium is carried out in the person and access media settings.

Time profile:
selection of the office mode time profile

Logging:
determination of the access event record type and data recording duration

Manual office mode:
manual office mode is active or not active

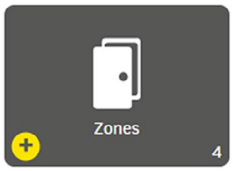
Shop mode:
shop mode is active or not active



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



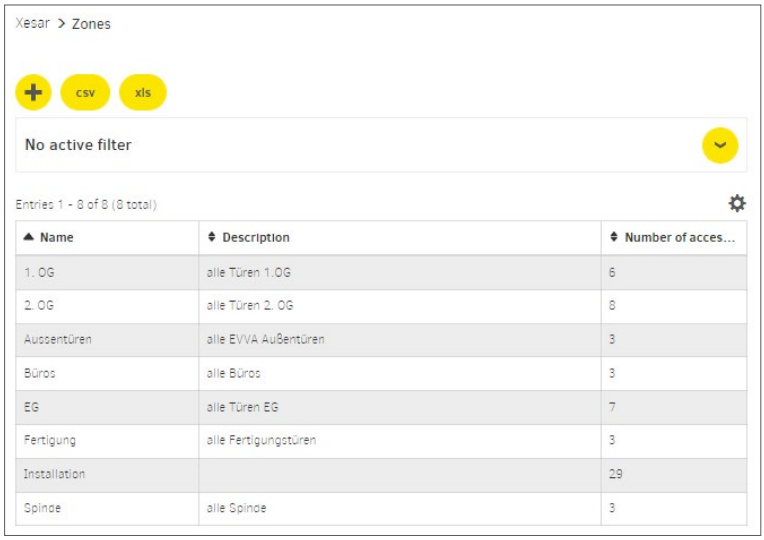
Access points can be merged into areas. This is useful if several access points have the same characteristics, e.g. the same authorisations, organisational affiliation, such as departments or building sections.

A maximum of 95 areas can be freely defined for each system (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.



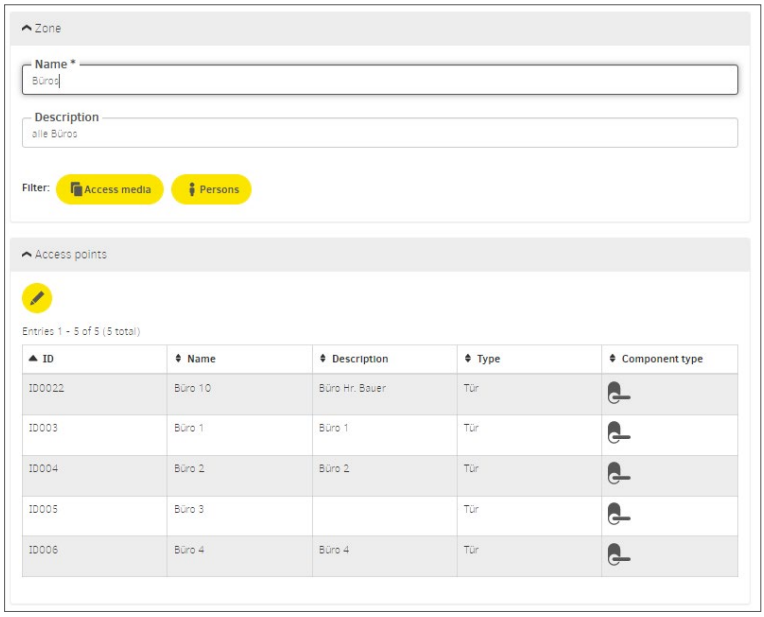
Name	Description	Number of acces...
1. OG	alle Türen 1.OG	6
2. OG	alle Türen 2. OG	8
Aussentüren	alle EVVA Außentüren	3
Büros	alle Büros	3
EG	alle Türen EG	7
Fertigung	alle Fertigungstüren	3
Installation		29
Spinde	alle Spinde	3

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

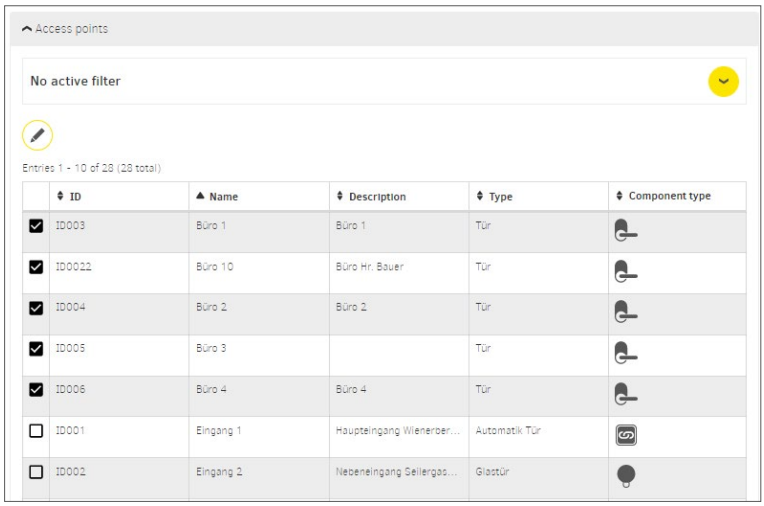
Name:
name of the area

Description:
supplementary information relating to the name

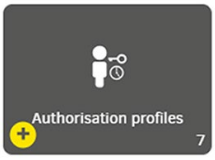
Access points:
shows the selected access points



Select access points:
Select the access points for the area in the first column.



2.9 Authorisation profiles

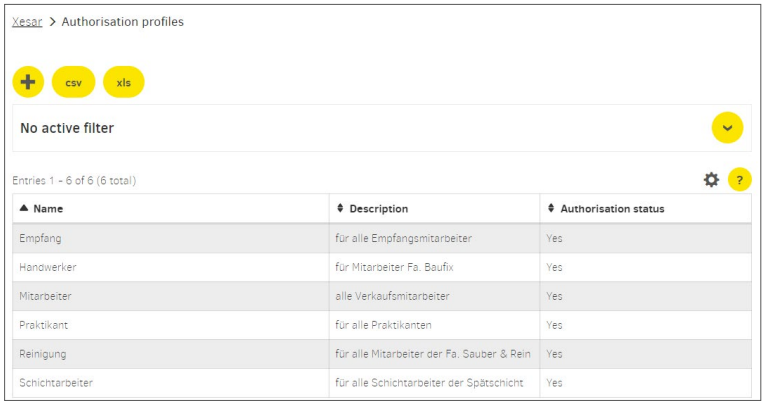


Authorisation profiles describe spatial and temporal access restrictions for access media. These access media can be assigned to persons. This means that a person with an access medium only has access to the access points and areas defined in the authorisation profile and only at the defined times. In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

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, for example, for access to lockers.)

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



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 *.

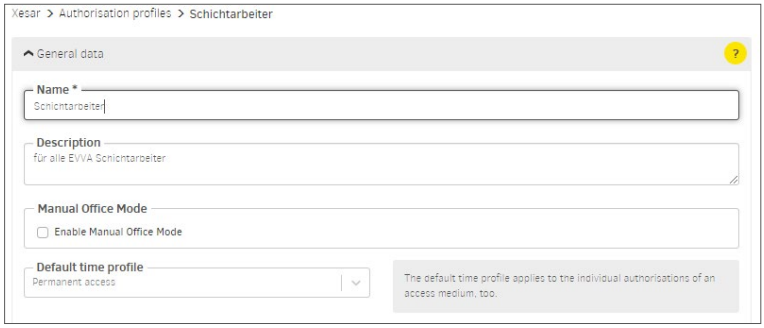
Name:
Name of the authorisation profile, e.g. shift worker

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

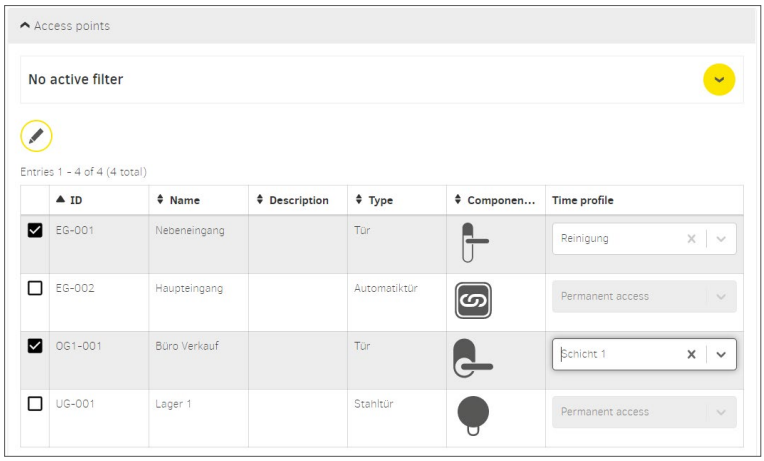
Manual office mode:
If manual office mode is activated, all persons or access media have the authorisation to activate manual office mode at the authorised access components.

Default time profile:
Selection from the time profiles

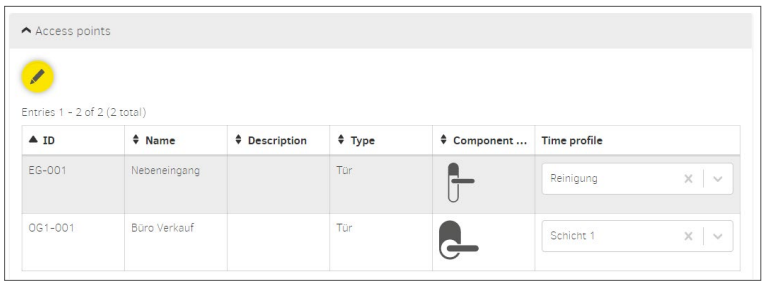
The default time profile may only use time profiles with a maximum of 12 time slots.



Selection of access points:



Access to the selected access points:

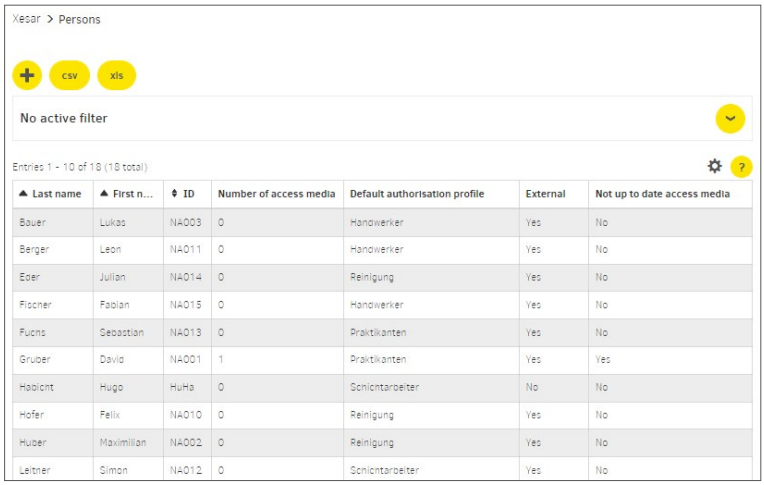


2.10 Persons

The “Persons” area defines all relevant information on the persons authorised in the system. Persons in a system 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).

Persons list display:



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
Hablcht	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 person’s code, e.g. initials

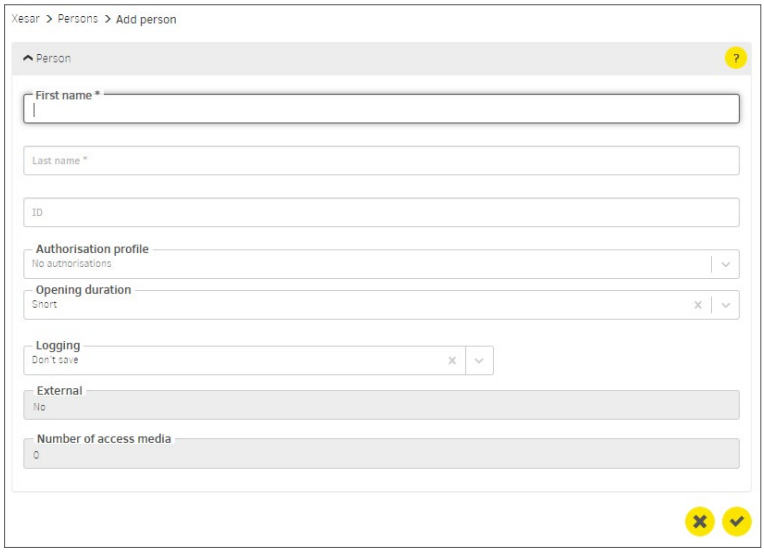
Number of access media:
The number of assigned access media for the person

Default 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 up to date 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 **Access media not up to date** on the dashboard is shown as yellow.)
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



Mandatory fields are marked with *.

First name:
The person's first name

Last name:
The person's last name

ID:
The person's code, e.g. initials

Authorisation profile:
Selection from the authorisation profiles; is written to the access medium, which is assigned to the person, as the default authorisation profile.

Opening duration:
The opening duration is **Short** or **Long** is activated on the access component if access is authorised.

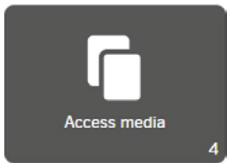
Logging:
Type of event recording – accesses can be either: not recorded, indefinitely recorded or recorded for a limited period of time.

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 assigned access media for the person

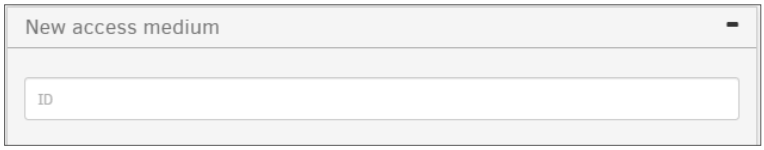
2.11 Access media



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).

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)

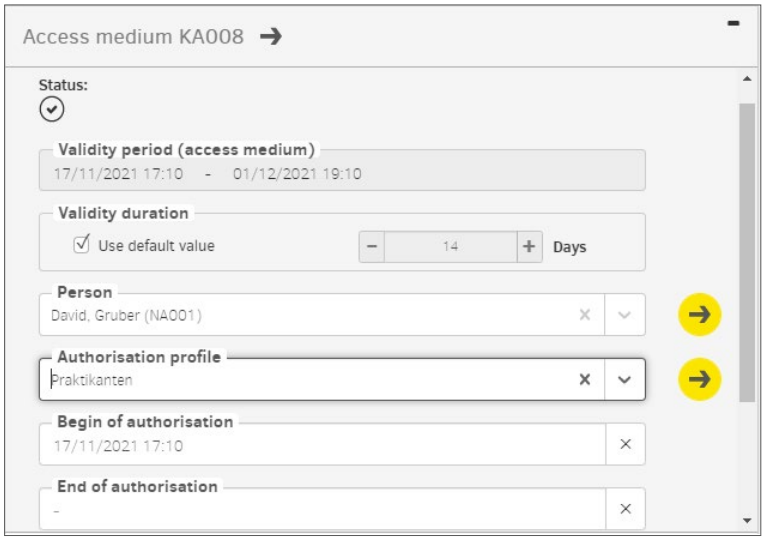
You can assign the access medium an access medium description (e.g. Hans Huber garage, visitor 1 or room 23).

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 contain any personal reference, e.g. Hans Huber.
This labelling is the responsibility of the user who assigns 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 until the access medium must be updated again at the Xesar online wall reader or the 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.
- **Customised:**
  enter 1 day to max. 7300 days (about 20 years)

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

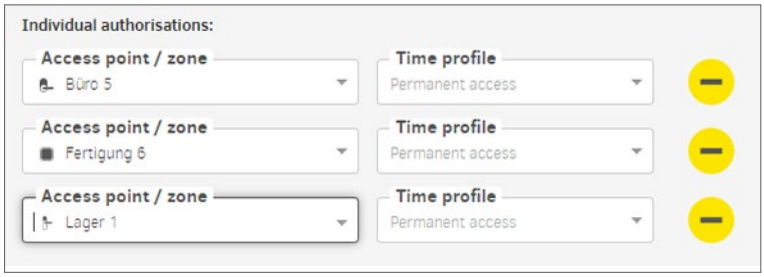
Access medium (substitute access medium) – The field only appears with a new access medium:
To create a substitute access medium, select the access medium of the person selected above with their authorisation profile here.

Authorisation profile:
Selection of the desired authorisation profile

Begin of authorisation:
Time for the begin of authorisation for the access medium. 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 internship).
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.
Three access points or areas each with a different time profile can be defined.



2.11.2 Existing access medium

After laying an existing access medium on the coding station, 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 is not authorised
4	Currently valid		
5	Currently invalid		

#	Status	Visualisation	Explanation
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		
8	Currently invalid access medium, which has a validity interval that lies in the future		
9	Deactivated access medium		The access medium has been deactivated. There are no further unsafe access points and the calendar no longer plays a role

Validity interval:
Selection of the time interval until the access medium must be updated again at the Xesar online wall reader or the coding station (validity is extended).

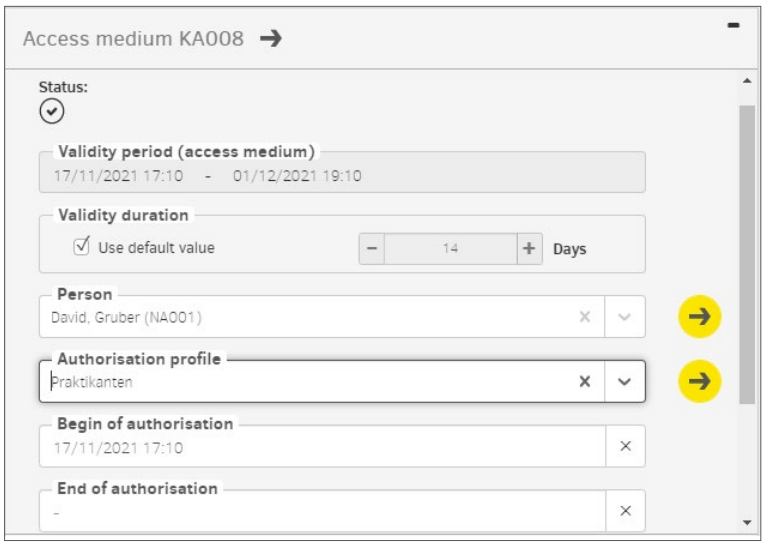
Validity duration:
Information regarding the period for which the access medium is valid.

- **Default value:**
  is defined in the general security settings.
- **Customised:**
  enter 1 day to max. 7300 days (about 20 years).

Person:
Person to whom this access medium is assigned.

Begin of authorisation:
From this point in time, the access medium is valid and authorised for authorisation updating.

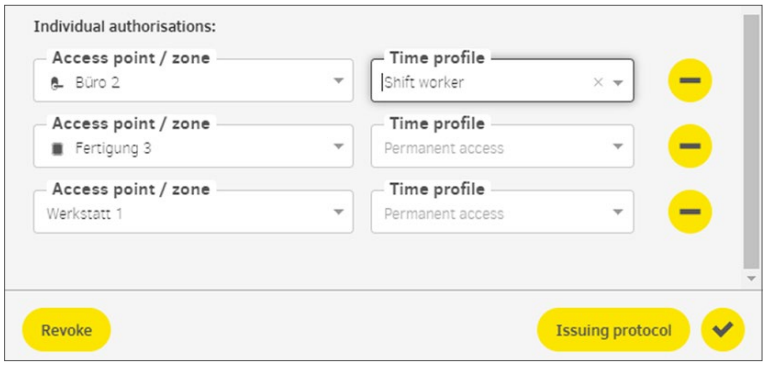
End of authorisation:
From this point in time, the access medium is no longer valid or authorised for authorisation updating.



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).

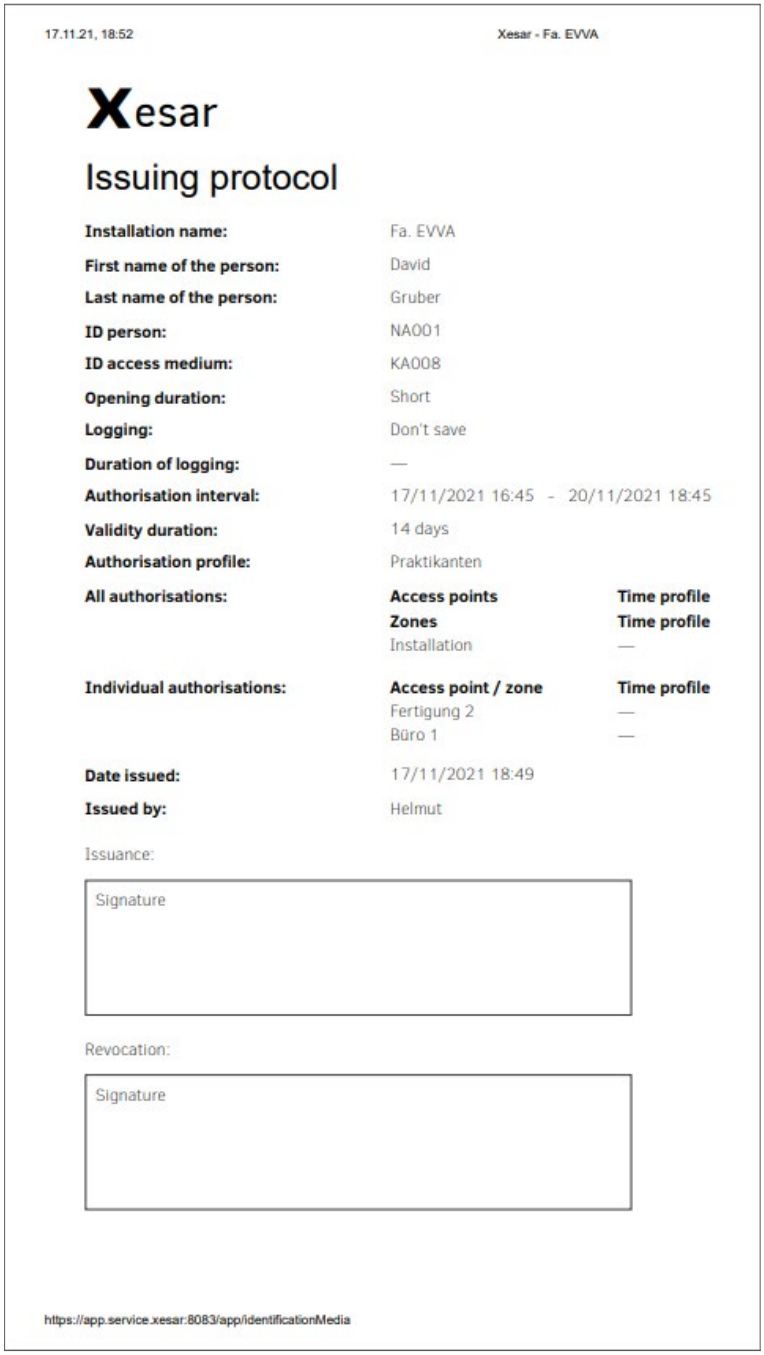
Withdraw:
Click on the **Withdraw** button to revoke the access medium. All settings except the identification number are deleted. (The function is used, e.g. for access media of employees who leave the company.)

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 confirmed by the recipient's signature when taking over 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 Adding 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 3.1, 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.

www.evva.com