EVVA
access to security

Xesar

Systemhandbuch Xesar 3.1

Impressum

Produktcode: I.TD.HDB.X.R3-1.SDE | 23R2

Version: Xesar 3.1 | 3.1.x
Ausgabe: 05/2023 DE
Originalbetriebsanleitung

Herausgeber
EVVA Sicherheitstechnologie GmbH

Für den Inhalt verantwortlich
EVVA Sicherheitstechnologie GmbH

Mit dem Erscheinen eines neuen Handbuchs verliert diese Ausgabe seine Gültigkeit.

Die aktuelle Ausgabe erhalten Sie im Downloadbereich von EVVA:

❯ **https://www.evva.com/at-de/service/downloads/**

Für Fehler technischer oder drucktechnischer Art und ihre Folgen übernehmen wir keine Haftung. Die Angaben in diesem Handbuch werden jedoch regelmäßig überprüft und Korrekturen vorgenommen.

Alle Warenzeichen und Schutzrechte werden anerkannt, Änderungen im Sinne des technischen Fortschritts können ohne Vorankündigungen vorgenommen werden.

Inhaltsverzeichnis

1 Einleitung

Das vorliegende Systemhandbuch beinhaltet Informationen zur Bedienung der Xesar-Software und der Xesar-Systemkomponenten.

Die im Xesar-Systemhandbuch beschriebenen Produkte/Systeme dürfen nur von Personen betrieben werden, die für die jeweiligen Aufgabenstellungen qualifiziert sind. Qualifiziertes Personal ist aufgrund seines Know-hows befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

1.1 Allgemeine rechtliche Hinweise

EVVA schließt den Vertrag zur Nutzung von Xesar auf Basis der EVVA-AGB (Allgemeine Geschäftsbedingungen) sowie EVVA-ALB (Allgemeine Lizenzbedingungen) für die Software zum Produkt ab.

Die EVVA-AGB und EVVA-ALB können Sie abrufen:

› **https://www.evva.com/at-de/impressum**

Beachten Sie, dass der Einsatz von Xesar gesetzliche, insbesondere datenschutzrechtliche Genehmigungs-, Melde- und Registrierungspflichten (zum Beispiel, wenn ein Informationsverbundsystem entsteht) sowie, bei Einsatz in Unternehmen, Mitbestimmungsrechte der Belegschaft auslösen kann. Die Verantwortung für den rechtskonformen Einsatz des Produktes liegt beim Betreiber.

Die vorstehenden Informationen sind gemäß der im Produkthaftungsgesetz definierten Haftung des Herstellers für seine Produkte zu beachten und müssen an die Betreiber und Nutzer weitergegeben werden. Die Nichtbeachtung entbindet EVVA von der Haftpflicht.

Die nicht verwendungsgemäße Benutzung sowie von EVVA nicht zugelassene Reparaturarbeiten bzw. Modifikationen und nicht fachgerechter Service können zu Funktionsstörungen führen und sind daher zu unterlassen. Änderungen, die nicht von EVVA ausdrücklich zugelassen sind, führen zum Verlust von Haftungs-, Gewährleistungs- und gesondert vereinbarten Garantieansprüchen.

Halten Sie die Systemkomponenten von Kleinkindern und Haustieren fern. Erstickungsgefahr durch verschluckbare Kleinteile.

Für **Architekten und beratende Institutionen** stellt EVVA alle erforderlichen Produktinformationen zur Verfügung, damit sie ihren Informations- und Instruktionspflichten gemäß Produkthaftungsgesetz nachkommen können.

Fachhändler und Verarbeiter müssen alle Hinweise in den EVVA-Dokumentationen beachten und diese bei Bedarf an ihre Kunden übermitteln.

Zusätzliche Informationen erhalten Sie im Produktkatalog von EVVA:

› **https://www.evva.com/at-de/xesar**

1.2 EVVA-Support

Mit Xesar steht Ihnen ein ausgereiftes und geprüftes Schließsystem zur Verfügung. Wenn Sie zusätzlich Unterstützung benötigen, wenden Sie sich bitte direkt an Ihren EVVA-Partner.

Die Liste zertifizierter EVVA-Partner können Sie hier abrufen:

› **https://www.evva.com/at-de/haendlersuche/**

Aktivieren Sie die Filter-Option „Elektronik-Partner", um gezielt nach EVVA-Partnern, die elektronische EVVA-Schließsysteme vertreiben und über ein qualifiziertes Fachwissen verfügen, zu suchen.

› **https://www.evva.com/de/xesar/support/**

Allgemeine Informationen zu Xesar können Sie hier abrufen:

› **https://www.evva.com/at-de/xesar**

1.3 Zeichenerklärung

Folgende Zeichen werden im Systemhandbuch zur besseren Darstellung verwendet:

Symbol	Bedeutung
	Achtung, Gefahr eines Sachschadens, wenn die entsprechenden Vorsichtsmaßnahmen nicht eingehalten werden
	Hinweise und zusätzliche Informationen
	Tipps und Empfehlungen
	Vermeiden bzw. Fehlermeldungen
Option	Optionen
	Links
	Schritt bei Handlungsanweisungen

1.2 Zeichenerklärung Xesar-Software

Folgende Zeichen werden in der Xesar-Software, im Installation-Manager und im Periphery-Manager verwendet:

1.2.1 Allgemein

#	Zustand	Symbol	Erklärung
1	Bestätigen / Speichern		Bestätigen oder Speichern von Eingaben
2	Hinzufügen		Hinzufügen von z. B. einer neuen Person oder Einbauort
3	Eingabe verwerfen		Verwerfen einer Eingabe
4	Entfernen		Entfernen von z. B. einer Anlage, Zeitprofil oder Einbauort
5	Bearbeiten		Bearbeiten der Anlage (Installation-Manager)
6	Anwendung starten		Starten der Anlage (Installation-Manager) oder Starten der Verbindung zwischen Codierstation und Xesar-Software (Periphery-Manager)
7	Anwendung stoppen		Stoppen der Anlage (Installation-Manager) oder Stoppen der Verbindung zwischen Codierstation und Xesar-Software (Periphery-Manager)
8	Download		Download von z. B. Supportinformationen
9	Weiter		Weiter zur nächsten Eingabe
10	Laden / Übertragen		Laden der Admin-Karte
11	Filtern		Anzeige möglicher Filter-Einstellungen der Funktion
12	Aktualisieren / Verbinden		Am Dashboard wird im Backend eine Aufgabe durchgeführt

#	Zustand	Symbol	Erklärung
13	Nicht aktualisiert / Warten auf Aktualisierung / Update down-loaden		Ein Update ist verfügbar und kann heruntergeladen werden
14	Suchen		Suchen nach einem speziellen Ereignisbeitrag
15	Ausklappen		Das Sichtfeld erweitern
16	Einklappen		Das Sichtfeld reduzieren
17	Gehe zu		Das Browserfenster für die Xesar-Software öffnen
18	Systemprotokoll		Alle Aktionen anzeigen, die in der Xesar-Soft-ware von Benutzern und vom System durch-geführt worden sind
19	Gefiltert nach Bereichen		Zeigt alle Bereiche an, zu welchen eine Per-son eine Zutrittsberechtigung hat
20	Gefiltert nach Einbauorten		Zeigt alle Einbauorte an, zu welchen eine Person eine Zutrittsberechtigung hat
21	Gefiltert nach Zutrittsmedien		Zeigt alle Zutrittsmedien an, die einer Person zugewiesen sind
22	Gefiltert nach Personen		Filtern nach Personen
23	Mein Profil		Mein Benutzerprofil bearbeiten: Beschreibung hinzufügen und persönliches Passwort ändern
24	Angezeigte Sprache		Spracheinstellung ändern
25	Anzeige Stück KeyCredits		Anzeige der abzubuchenden KeyCredits (z. B. durch Berechtigungsänderungen oder Ausgabe von neuen Zutrittsmedien)
26	Anzeige KeyCredit Lifetime		Wird angezeigt, wenn KeyCredit Lifetime ein-gelöst wurde
27	Ereignisprotokoll		Anzeige Ereignisse, z. B. unter einer Person (es werden alle Zutrittsereignisse der Person gefiltert angezeigt)

#	Zustand	Symbol	Erklärung
28	Hilfetexte		Anzeige von Hilfetexten
29	Listenexport		Die angezeigte Liste als csv-Datei oder als xls-Datei exportieren
30	Listenansichtseinstellung		Darstellung der Liste anpassen (Spaltenauswahl, Zeilenanzahl pro Seite, Einstellungen speichern und Rücksetzen)
31	Backup-Button		Im Installation-Manager wird ein Backup der Anlagendaten erstellt
32	Logout		Sitzung beenden
33	Batterie voll		Batterie ist voll
34	Batteriewarnung		Batterie ist leer; tauschen Sie ehestens die Batterien aus
35	Komponente mit Kabel-Schnittstelle		Zutrittskomponenten, die nur mit Kabelverbindung zum Tablet synchronisiert werden können
36	Komponente mit drahtloser BLE-Schnittstelle; BLE ist aktiviert		Zutrittskomponenten, die mit drahtloser BLE- und mit Kabelverbindung zum Tablet synchronisiert werden können; BLE-Funktion der Zutrittskomponente ist aktiviert
37	Komponente mit drahtloser BLE-Schnittstelle; BLE ist deaktiviert		Zutrittskomponenten, die mit drahtloser BLE- und mit Kabelverbindung zum Tablet synchronisiert werden können; BLE-Funktion der Komponente ist deaktiviert
38	Warnung		z.B. es sind noch unsichere Einbauorte vorhanden

1.2.2 Zustände Zutrittsmedien

#	Zustand	Visualisierung	Erklärung
1	Unsicher gesperrtes Zutrittsmedium		Das Zutrittsmediium ist gesperrt. Es sind noch unsichere Einbauorte vorhanden. Bringen Sie die Blacklist mit dem Tablet oder einem aktualisierten Zutrittsmedium zu den unsicheren Einbauorten.
2	Sicher gesperrtes Zutrittsmedium		Das Zutrittsmedium ist gesperrt. Es sind keine unsicheren Einbauorte vorhanden. Die Anlage ist sicher.
3	Unberechtigtes Zutrittsmedium		Das Zutrittsmedium verfügt über keine Berechtigung. Grund z. B. der Berechtigungszeitraum wurde überschritten.
4	Aktuell gültig		Das Zutrittsmedium ist gültig und kann laut Berechtigungsprofil verwendet werden.
5	Aktuell ungültig		Das Zutrittsmedium ist aktuell ungültig.
6	Aktuell gültiges Zutrittsmedium wird bei Aktualisierung zu einem ungültigen Zutrittsmedium		Das Zutrittsmedium ist aktuell gültig. Es wird aber nach einer Aktualisierung am Online-Wandleser oder an der Codierstation ungültig.
7	Aktuell ungültiges Zutrittsmedium wird bei Aktualisierung zu einem gültigen Zutrittsmedium		Das Zutrittsmedium ist aktuell ungültig. Es wird aber nach einer Aktualisierung am Online-Wandleser oder an der Codierstation gültig.
8	Aktuell ungültiges Zutrittsmedium mit einem Gültigkeitsintervall auf dem Zutrittsmedum, das in der Zukunft liegt		Das Zutrittsmedium ist aktuell ungültig. Es bleibt auch nach einer Aktualisierung am Online-Wandleser oder an der Codierstation ungültig.
9	Deaktiviertes (gesperrtes) Zutrittsmedium		Das Zutrittsmedium wurde deaktiviert; es gibt keine unsicheren Einbauorte mehr; der Kalender spielt keine Rolle mehr.

2 Hardware und Montage

Prüfen Sie, ob das ausgewählte Xesar-Produkt für die von Ihnen vorgesehene Anwendung geeignet ist und beachten Sie die Hinweise im entsprechenden Datenblatt.

› **https://www.evva.com/at-de/xesar/**

Systemarchitektur (Symbolfoto)

2.1 Zutrittskomponenten

Die Vielfältigkeit von Xesar bietet verschiedene Komponenten, wie unterschiedliche Formen von Beschlag, Drücker, Zylinder (u. a. Hybrid- und Hebelzylinder), Wandleser und Hangschloss.

Beschlag

Drücker

Zylinder

Hangschloss

Wandleser

Zutrittskomponenten der Generation G2.0 haben eine blaue oder grüne Farbmarkierung unter dem EVVA-Logo (Stecker-Abdeckung). Sie haben nur eine Stecker-Schnittstelle zur Synchronisation mit dem Tablet.

Zutrittskomponenten der Generation G2.1 sind an der gelben Farbmarkierung unter dem EVVA-Logo (Stecker-Abdeckung) erkennbar.
Sie verfügen über eine Drahtlos- und eine Stecker-Schnittstelle, die zur Aktualisierung mit dem Tablet dienen. Die Drahtlos-Schnittstelle kann ab der Xesar-Version 3.1 und ab der Tablet-Version Ares BLE 4.2 verwendet werden.

Die Stecker-Schnittstelle kann bei batteriebetriebenen Zutrittskomponenten bei Bedarf auch für die Notstromversorgung benutzt werden.

Ab der Xesar-Version 3.1 können die Zutrittskomponenten der Generation G2.1 mit dem Tablet Ares BLE 4.2 zusätzlich zur kabelgebundenen Schnittstelle auch über die drahtlose BLE-Schnittstelle synchronisiert und gewartet werden.
Alle Synchronisations- und Wartungsaufgaben, wie Konfigurationsänderungen, Ereignisdaten-Synchronisation oder Firmwareupdates können an allen in Reichweite befindlichen Zutrittskomponenten nach erfolgreicher Verbindung durchgeführt werden.
Siehe dazu auch Kapitel „Wartungsaufgaben mit Tablet durchführen".

Verwenden Sie KEINE spitzen Gegenstände, um die Stecker-Abdeckung zu öffnen!

» Drücken Sie leicht auf den Buchstaben E des EVVA-Schriftzugs.
» Klappen Sie beim Buchstaben A des EVVA-Schriftzugs die Stecker-Abdeckung nach vorne.

Schließen Sie die Stecker-Abdeckung nach Gebrauch wieder, um die Stecker-Schnittstelle vor Staub und Feuchtigkeit zu schützen!

Lagern Sie Batterien an einem kühlen, trockenen Ort. Direkte starke Wärme kann die Batterien beschädigen. Setzen Sie Ihre batteriebetriebenen Geräte daher keinen starken Hitzequellen aus.

Batterien enthalten chemische Substanzen, sie müssen deshalb unter Berücksichtigung der landesspezifischen Vorschriften fachgerecht entsorgt werden.

2.1.1 Beschlag

- Batteriebetriebene Zutrittskomponente
- Einsatz im Außen- und Innenbereich
- Geeignet für gängige Rohrrahmen- und Vollblatttürschlösser mit Drückerwinkel bis zu 40° mit selbstverriegelnden Fluchttürschlössern nach EN 179/EN 1125, Feuerschutztüren und – in entsprechender Ausführung – Panik- und Fluchttüren mit Stangengriffen oder Druckstangen nach EN 1125

Beachten Sie die mitgelieferten Sicherheitstexte, die zusätzlich wichtige Informationen zu Montage, Gebrauch und Wartung der Zutrittskomponenten beinhalten.

› **https://www.evva.com/at-de/xesar/**

Verwenden Sie in Außen- oder Nassbereichen die dafür vorgesehene Dichtung, die dem Produkt beiliegt.

Beachten Sie bei der Montage auf Brandschutztüren, dass die Zertifikate ausschließlich mit den Freigaben der jeweiligen Türhersteller gelten.

Beschlag (Symbolfoto)

1. Optische Signalisierung
2. Leseeinheit
3. Stecker-Schnittstelle (EVVA-Logo)
   Farbmarkierung (BLE oder 3-Zack) unter dem EVVA-Logo
4. Drücker

Der Sensor der Leseeinheit befindet sich an der Außenseite des Beschlags, zwischen der Stecker-Schnittstelle und der optischen Signalisierung (LED).

Der Beschlag signalisiert Ereignisse sowohl akustisch als auch optisch.
Beachten Sie die Liste der unterschiedlichen akustischen und optischen Signale im Kapitel „Ereignissignalisierung".

Der Beschlag verfügt über eine Dauerfreigabe-Funktion. Beachten Sie dazu die Hinweise zur Dauerfreigabe-Funktion.

Funktionsprinzip

Der Außendrücker ist standardmäßig ausgekuppelt, bei Betätigung des Außendrückers bleibt die Position der Falle unverändert.

Wird ein berechtigtes Zutrittsmedium an der Leseeinheit vorgehalten, wird der Außendrücker für 5 Sekunden mechatronisch eingekuppelt. Wird jetzt der Außendrücker betätigt, wird die Falle bzw. der Riegel – abhängig von der Schlosstype – mitgenommen.

Der Innendrücker ist immer eingekuppelt und kann jederzeit betätigt werden. Die Falle wird dabei stets mitgenommen.

Ereignisspeicher

Im Ereignisspeicher werden bis zu 1.000 Ereignisse gespeichert. Wenn der Ereignisspeicher voll ist, werden die Einträge der ältesten Ereignisse überschrieben.

Synchronisieren Sie die Ereignisse regelmäßig!
Damit verhindern Sie, dass protokollierte Ereignisse überschrieben werden.

Informationen zu weiteren Spezifikationen entnehmen Sie dem Datenblatt.

https://www.evva.com/at-de/xesar/

Batteriewechsel

Nicht rechtzeitig gewechselte Batterien können zum Ausfall des Beschlags führen!

Der Beschlag kann bei leeren Batterien nur mit dem Notstromgerät (optionales Zubehör) und einem Generalhauptschlüssel- oder Feuerwehr-Medium betätigt werden.

Wenn an der Zutrittskomponente „Batterie leer" angezeigt wird, müssen die Batterien umgehend gewechselt werden. (Siehe dazu auch Kapitel „Ereignissignalisierung".)
Wenn das Signal „Batterie leer" das erste Mal angezeigt wird, sind für einen Zeitraum von 4 Wochen maximal 1.000 Öffnungen möglich. Die Anzahl der Öffnungen ist abhängig von der Raumtemperatur und kann entsprechend geringer sein.

Lassen Sie die Batterien nur von geschultem Fachpersonal wechseln!

Das Batteriefach befindet sich im oberen Bereich des Innenschildes.
Für den Batteriewechsel benötigen Sie drei Batterien (Type AAA) und einen Torx-Schraubendreher T8.

Tauschen Sie beim Batteriewechsel immer alle 3 Batterien (Type AAA). Eine Liste der empfohlenen Batteriemodelle erhalten Sie auf Anfrage bei Ihrem Fachhändler.

Die Verwendung von Akkumulatoren (Akkus) ist unzulässig!

Wenn der Batteriewechsel – die Stromunterbrechung – länger als eine Minute dauert, muss der Beschlag mit dem Tablet synchronisiert werden!

Der Batteriewechsel des Beschlags für Paniktüren funktioniert analog. (Nur das Aussehen des Innenbeschlags weicht ab.)

Um die Batterien zu wechseln, gehen Sie wie folgt vor:

» Lösen Sie das Innenschild.
Lösen Sie die Schraube an der Unterseite des Beschlags mit einem Torx-Schraubendreher T8. Drehen Sie die Schraube im Uhrzeigersinn so weit hinein, bis Sie das Innenschild lösen können.
» Nehmen Sie das Innenschild ab.
Greifen Sie das Innenschild an seiner Unterseite und ziehen Sie es vorsichtig vom Befestigungsblech ab. Ziehen Sie das Innenschild über den Drücker. **Achten Sie darauf**, dass der Drücker nicht zerkratzt wird. (Alternativ können Sie im Vorfeld den Innendrücker abnehmen.)
» Wechseln Sie alle Batterien. **Achten Sie darauf**, dass die Batterien lagerichtig eingelegt werden!

Der erfolgreiche Batteriewechsel wird mit „Batterie eingelegt bzw. Reboot der Komponente" signalisiert!
Beachten Sie dazu das Kapitel „Ereignissignalisierung".

» Setzen Sie das Innenschild wieder auf das Befestigungsblech.
» Schieben Sie das Innenschild über den Drücker.
» Ziehen Sie die Schraube an der Unterseite des Beschlags mit einem Torx-Schraubendreher T8 an.
» Nach erfolgreichem Batterietausch synchronisieren Sie die Komponente mit dem Tablet und der Xesar-Software. Dadurch wird der neue Batteriestatus in die Xesar-Software übertragen.

2.1.2 Drücker

- Batteriebetriebene Zutrittskomponente
- Einsatz im Innenbereich
- Geeignet für Vollblatttüren mit gängigen Vollblatttürschlössern mit Drückerwinkel bis zu 40°, Fluchttürschlösser nach EN 179, Feuerschutztüren und Glastüren in Verbindung mit entsprechendem Glastürschloss
- Aufgrund der Einhaltung wesentlicher Schlossnormen und Drückerwinkel bis zu 40° mit vielen europäischen Schlössern kompatibel

Beachten Sie die mitgelieferten Sicherheitstexte, die zusätzlich wichtige Informationen zu Montage, Gebrauch und Wartung der Zutrittskomponenten beinhalten.

› **https://www.evva.com/at-de/xesar/**

Beachten Sie bei der Montage auf Brandschutztüren, dass die Zertifikate ausschließlich mit den Freigaben der jeweiligen Türhersteller gelten.

Drücker (Symbolfoto)

1. Optische Signalisierung
2. Leseeinheit
3. Stecker-Schnittstelle (EVVA-Logo)
   Farbmarkierung (BLE oder 3-Zack) unter dem EVVA-Logo
4. Drücker mit Batteriefach

Der Sensor der Leseeinheit befindet sich an der Außenseite des Drückers, zwischen der Stecker-Schnittstelle und der optischen Signalisierung (LED).

Der Drücker signalisiert Ereignisse sowohl akustisch als auch optisch.

Beachten Sie die Liste der unterschiedlichen akustischen und optischen Signale im Kapitel „Ereignissignalisierung".

Der Drücker verfügt über eine Dauerfreigabe-Funktion. Beachten Sie dazu die Hinweise zur Dauerfreigabe-Funktion.

Funktionsprinzip

Der Außendrücker ist standardmäßig ausgekuppelt, bei Betätigung des Außendrückers bleibt die Position der Falle unverändert.

Wird ein berechtigtes Zutrittsmedium an der Leseeinheit vorgehalten, wird der

Außendrücker für 5 Sekunden mechatronisch eingekuppelt. Wird jetzt der Außendrücker betätigt, wird die Falle bzw. der Riegel – abhängig von der Schlosstype – mitgenommen.

Der Innendrücker ist immer eingekuppelt und kann jederzeit betätigt werden. Die Falle wird dabei stets mitgenommen.

Ereignisspeicher

Im Ereignisspeicher werden bis zu 1.000 Ereignisse gespeichert. Wenn der Ereignisspeicher voll ist, werden die Einträge der ältesten Ereignisse überschrieben.

Synchronisieren Sie die Ereignisse regelmäßig!
Damit verhindern Sie, dass protokollierte Ereignisse überschrieben werden.

Informationen zu weiteren Spezifikationen entnehmen Sie dem Datenblatt.

https://www.evva.com/at-de/xesar/

Batteriewechsel

Nicht rechtzeitig gewechselte Batterien können zum Ausfall des Drückers führen!

Der Drücker kann bei leeren Batterien nur mit dem Notstromgerät (optionales Zubehör) und einem Generalhauptschlüssel- oder Feuerwehr-Medium betätigt werden.

Wenn Signal „Batterie leer" angezeigt wird, müssen die Batterien umgehend gewechselt werden. (Wenn das Signal „Batterie leer" das erste Mal angezeigt wird, sind für einen Zeitraum von 4 Wochen maximal 1.000 Öffnungen möglich. Die Anzahl Öffnungen ist abhängig von der Raumtemperatur und kann entsprechend geringer sein.)

Beachten Sie die Liste der unterschiedlichen akustischen und optischen Signale im Kapitel „Ereignissignalisierung".

Lassen Sie die Batterien nur von geschultem Fachpersonal wechseln!

Das Batteriefach befindet sich im Außendrücker des Drückers.
Für den Batteriewechsel benötigen Sie eine Batterie (Type CR123A) und einen Inbusschlüssel 2,5.

Eine Liste der empfohlenen Batteriemodelle erhalten Sie auf Anfrage bei Ihrem Fachhändler.

Die Verwendung von Akkumulatoren (Akkus) ist unzulässig!

Wenn der Batteriewechsel – die Stromunterbrechung – länger als eine Minute dauert, muss der Drücker mit dem Tablet synchronisiert werden!

Um die Batterien zu wechseln, gehen Sie wie folgt vor:

» Nehmen Sie das Drückerrohr des Außendrückers ab.
Drehen Sie mit dem Inbusschlüssel die Befestigungsschraube im Uhrzeigersinn hinein, bis sich das Drückerrohr abnehmen lässt. **Achten Sie darauf**, dass die Befestigungsschraube nur so weit wie nötig hineingedreht wird.
» Wechseln Sie die Batterie. **Achten Sie darauf**, dass die Batterie lagerichtig eingelegt wird!

Der erfolgreiche Batteriewechsel wird mit „Batterie eingelegt bzw. Reboot der Komponente" signalisiert!
Beachten Sie die Liste der unterschiedlichen akustischen und optischen Signale im Kapitel „Ereignissignalisierung".

» Setzen Sie das Drückerrohr wieder auf den Außendrücker.
Drehen Sie mit dem Inbusschlüssel die Befestigungsschraube gegen den Uhrzeigersinn heraus, um das Drückerrohr zu befestigen. **Achten Sie darauf**, dass die Befestigungsschraube nur so weit wie nötig hinausgedreht wird

» Nach erfolgreichem Batterietausch synchronisieren Sie die Komponente mit dem Tablet und der Xesar-Software. Dadurch wird der neue Batteriestatus in die Xesar-Software übertragen.

2.1.3 Zylinder

- Batteriebetriebene Zutrittskomponente
- Einsatz im Außen- und Innenbereich
- Geeignet für Brandschutz- und Fluchttüren
- Bereits in der Standardausführung mit einer Vielzahl von Schutzmaßnahmen gegen Manipulation ausgestattet.
- Der Zylinder steht als Halb- oder Doppelzylinder, mit ein- oder beidseitiger elektronischer Freigabe zur Auswahl.

Beachten Sie die mitgelieferten Sicherheitstexte, die zusätzlich wichtige Informationen zu Montage, Gebrauch und Wartung der Zutrittskomponenten beinhalten.

› **https://www.evva.com/at-de/xesar/**

Beachten Sie bei der Montage auf Brandschutztüren, dass die Zertifikate ausschließlich mit den Freigaben der jeweiligen Türhersteller gelten.

Zylinder (Symbolfoto)

1. Optische Signalisierung
2. Leseeinheit
3. Stecker-Schnittstelle (EVVA-Logo)
   Farbmarkierung (BLE oder 3-Zack) unter dem EVVA-Logo

Der Sensor der Leseeinheit befindet sich in der Kunststoffkappe des Zylinders, zwischen der Stecker-Schnittstelle und der optischen Signalisierung (LED).

Der Zylinder signalisiert Ereignisse sowohl akustisch als auch optisch.
Beachten Sie die Liste der unterschiedlichen akustischen und optischen Signale im Kapitel „Ereignissignalisierung".

Der Zylinder verfügt über eine Dauerfreigabe-Funktion. Beachten Sie dazu die Hinweise zur Dauerfreigabe-Funktion.

Funktionsprinzip

Der elektronische Außenknauf des Zylinders ist standardmäßig ausgekuppelt; bei Betätigung des Außenknaufs bleibt die Sperrnase ausgekuppelt und der Außenknauf dreht, ohne die Sperrnase mitzunehmen.

Bei Zylindern mit einseitiger elektronischer Freigabe bleibt die mechanische Innenseite immer eingekuppelt und kann jederzeit betätigt werden.

Bei Zylindern mit beidseitiger elektronischer Freigabe verhält sich der elektronische Innenknauf analog zum elektronischen Außenknauf.

Wird ein berechtigtes Zutrittsmedium an der Leseeinheit vorgehalten, wird der Außenknauf für 5 Sekunden mechatronisch eingekuppelt. Die Sperrnase des Zylinders wird bei der Betätigung des Außenknaufs mitgenommen.

Die Tür wird nach dem Schließen NICHT automatisch verriegelt.
Die Verriegelung der Tür muss manuell oder über eine entsprechende zusätzliche Einrichtung erfolgen.

Das Drehverhalten des Knaufs kann unter Umständen durch Reibung der Dichtung am Beschlag bzw. an der Zylinderrosette des Zylinders schwergängiger sein. Im Innenbereich besteht in diesen Fällen die Möglichkeit, die Dichtung abzunehmen.

Der Zylinder ist standardmäßig mit einer Rotationsbremse ausgestattet. Zylinder mit Freilauffunktion (FZG) und Antipanik (FAP) verfügen aus technischen Gründen nicht über eine Rotationsbremse..

Achten Sie auf den lagerichtigen Einbau der Rotationsbremse, damit es im laufenden Betrieb zu keinen Fehlfunktionen kommt.
Fehlfunktionen in nicht freigegebenen Einbauanlagen sind kein Produktionsfehler und daher kein Reklamationsgrund.

Ereignisspeicher

Im Ereignisspeicher werden bis zu 1.000 Ereignisse gespeichert. Wenn der Ereignisspeicher voll ist, werden die Einträge der ältesten Ereignisse überschrieben.

Synchronisieren Sie die Ereignisse regelmäßig!
Damit verhindern Sie, dass protokollierte Ereignisse überschrieben werden.

Informationen zu weiteren Spezifikationen entnehmen Sie dem Datenblatt.

› **https://www.evva.com/at-de/xesar/**

Batteriewechsel

» Aktivieren Sie vor dem Batteriewechsel die Daueröffnung des Zylinders, damit der Zylinder eingekuppelt bleibt.

Der Betrieb des Zylinders ist nur mit Batterien der Type CR2 zulässig.

Eine Liste der empfohlenen Batteriemodelle erhalten Sie auf Anfrage bei Ihrem Fachhändler.

Die Verwendung von Akkumulatoren (Akkus) ist unzulässig!

Lassen Sie die Batterien nur von geschultem Fachpersonal wechseln!

Wenn Signal „Batterie leer" angezeigt wird, müssen die Batterien umgehend gewechselt werden. (Wenn das Signal „Batterie leer" das erste Mal angezeigt wird, sind für einen Zeitraum von 4 Wochen maximal 1.000 Öffnungen möglich. Die Anzahl Öffnungen ist abhängig von der Raumtemperatur und kann entsprechend geringer sein.)

Der Zylinder kann bei leeren Batterien nur mit dem Notstromgerät (optionales Zubehör) und einem Generalhauptschlüssel- oder Feuerwehr-Medium betätigt werden.

Tauschen Sie bei einem Batteriewechsel alle im Zylinder eingesetzten Batterien aus!

Verwenden Sie für die Montage bzw. Demontage des Knaufs (auch beim Batteriewechsel) das spezielle Montagewerkzeug für den Zylinder.

Wir empfehlen Ihnen, den Zylinder vor Entnahme der Batterien mittels eines berechtigten Zutrittsmediums einzukuppeln. Gegebenenfalls ist nach dem Austausch von Batterien eine Synchronisation der Systemuhrzeit über das Tablet erforderlich.

Um die Batterien des Zylinders zu wechseln, gehen Sie wie in der Montageanleitung angeführt, jedoch in umgekehrter Reihenfolge, vor.

» Setzen Sie das Zylinderwerkzeug vollständig auf die dafür vorgesehene Ausnehmung auf der Rückseite des Außenknaufs und schrauben Sie den Knauf und das Werkzeug gemeinsam (gegen den Uhrzeigersinn) herunter.

» Entfernen Sie das Zylinderwerkzeug und öffnen Sie die 3 Befestigungsschrauben mit einem Kreuzschraubendreher (PH1) auf der Rückseite des Außenknaufs.

» Nehmen Sie die Knaufscheibe ab.

» Öffnen Sie vorsichtig den Verschluss im Außenknauf, indem Sie diesen vorsichtig verschieben und dann aufklappen.

» Entnehmen Sie die beiden leeren Batterien CR2 und reinigen Sie die Batteriekontakte mit einem weichen, fusselfreien Tuch.

» Setzen Sie die beiden neuen Batterien lagerichtig in das Batteriefach ein und verschließen Sie dieses wieder.

Wenn der Batteriewechsel – die Stromunterbrechung – länger als eine Minute dauert, muss der Zylinder mit dem Tablet synchronisiert werden!

» Sollte der Batteriewechsel korrekt durchgeführt worden sein, erfolgt die Initialisierung und es ertönt die entsprechende Signalisierung. (Siehe Kapitel „Ereignissignalisierung", Signal 8 der Signalisierungstabelle).

» Setzen Sie die Knaufscheibe wieder auf und befestigen Sie sie mit den 3 Befestigungsschrauben.

» Setzen Sie das Zylinderwerkzeug auf der Rückseite des Außenknaufs vollständig auf und schrauben Sie den Knauf und das Werkzeug gemeinsam (im Uhrzeigersinn) auf den Zylinder, bis Sie einen Widerstand spüren.

» Drehen Sie den Zylinder anschließend in die entgegengesetzte Richtung (gegen den Uhrzeigersinn), bis Sie ein „Klick" hören.

» Nehmen Sie das Zylinderwerkzeug wieder ab.

» Nach erfolgreichem Batterietausch synchronisieren Sie die Komponente mit dem Tablet und der Xesar-Software. Dadurch wird der neue Batteriestatus in die Xesar-Software übertragen.

Knauf-Achse fixieren

Alle Zylinder in Europrofilausführung haben an der Stirnseite des Elektronikmoduls eine Servicebohrung. Um die Demontage des Zylinderknaufs zu erleichtern, fixieren Sie die Knauf-Achse mit einem passenden Metallstift.

Der Metallstift soll einen Durchmesser von 2 mm haben und mindestens 40 mm lang sein.

Um die Knauf-Achse zu fixieren, gehen Sie wie folgt vor:

» Führen Sie einen passenden Metallstift – z. B. einen Inbusschlüssel – 2 mm in den Servicekanal an der Stirnseite des Europrofilzylinders ein.

» Drehen Sie beim Einführen des Metallstiftes den Knauf so lange um die eigene Achse, bis sich der Metallstift merklich tiefer in den Servicekanal führen lässt.

» Halten Sie den Metallstift in dieser Position und demontieren Sie den Knauf wie gewohnt mit dem Montagewerkzeug.

» Entfernen Sie den Metallstift vorsichtig nach der Demontage des Knaufs.

2.1.4 Hybridzylinder

- Batteriebetriebene Zutrittskomponente
- Einsatz im Außen- und Innenbereich
- Bereits in der Standardausführung mit einer Vielzahl von Schutzmaßnahmen gegen Manipulation ausgestattet.
- Geeignet für Brandschutz- und Fluchttüren
  Für den Einsatz in Flucht- und Paniktüren kann – in Abhängigkeit vom verwendeten Einsteckschloss – die Antipanik-Funktion FAP erforderlich sein. Beachten Sie hierzu die entsprechenden Hinweise bzw. Zertifikate

Beachten Sie bei der Montage auf Brandschutztüren, dass die Zertifikate ausschließlich mit den Freigaben der jeweiligen Türhersteller gelten!

Hybridzylinder (Symbolfoto)

❶ Optische Signalisierung
❷ Leseeinheit
❸ Stecker-Schnittstelle (EVVA-Logo)
Farbmarkierung (BLE oder 3-Zack) unter dem EVVA-Logo

Der Sensor der Leseeinheit befindet sich in der Kunststoffkappe des Zylinders, zwischen der Stecker-Schnittstelle und der optischen Signalisierung (LED).

Der Zylinder signalisiert Ereignisse sowohl akustisch als auch optisch.
Beachten Sie die Liste der unterschiedlichen akustischen und optischen Signale im Kapitel „Ereignissignalisierung".

Der Zylinder verfügt über eine Dauerfreigabe-Funktion. Beachten Sie dazu die Hinweise zur Dauerfreigabe-Funktion.

Funktionsprinzip

Beim Hybridzylinder befindet sich an der Innenseite, an Stelle des mechanischen Knaufs, ein Schlüsselmodul. Das bedeutet: Der Zutritt von außen erfolgt über eine elektronische Berechtigungsprüfung und der Zutritt von innen über einen mechanischen Schlüssel.

Nach dem Schließen der Tür wird diese nicht automatisch verriegelt. Die Verriegelung der Tür muss manuell oder über eine entsprechende zusätzliche Einrichtung erfolgen.

Prüfen Sie, ob der ausgewählte Hybridzylinder Ihren Anforderungen entspricht. Informationen zu weiteren Spezifikationen entnehmen Sie dem Datenblatt.

› **https://www.evva.com/at-de/service/downloads/**

Der Hybridzylinder besitzt eine optische und eine akustische Signalisierung. (Erläuterungen der verschiedenen Signale siehe Kapitel „Ereignissignalisierung".)

Beachten Sie die mitgelieferte Montageanleitung.

Batteriewechsel

» Aktivieren Sie vor dem Batteriewechsel die Daueröffnung des Hybridzylinders, damit der Hybridzylinder eingekuppelt bleibt.

Der Betrieb des Zylinders ist nur mit Batterien der Type CR2 zulässig.

Eine Liste der empfohlenen Batteriemodelle erhalten Sie auf Anfrage bei Ihrem Fachhändler.

Die Verwendung von Akkumulatoren (Akkus) ist unzulässig!

Lassen Sie die Batterien nur von geschultem Fachpersonal wechseln!

Wenn Signal „Batterie leer" angezeigt wird, müssen die Batterien umgehend gewechselt werden. (Wenn das Signal „Batterie leer" das erste Mal angezeigt wird, sind für einen Zeitraum von 4 Wochen maximal 1.000 Öffnungen möglich. Die Anzahl Öffnungen ist abhängig von der Raumtemperatur und kann entsprechend geringer sein.)

Der Hybridzylinder kann bei leeren Batterien nur mit dem Notstromgerät (optionales Zubehör) und einem Generalhauptschlüssel- oder Feuerwehr-Medium betätigt werden.

Tauschen Sie bei einem Batteriewechsel alle im Zylinder eingesetzten Batterien aus!

Verwenden Sie für die Montage bzw. Demontage des Knaufs (auch beim Batteriewechsel) das spezielle Montagewerkzeug für den Zylinder.

Wir empfehlen Ihnen, den Zylinder vor Entnahme der Batterien mittels eines berechtigten Zutrittsmediums einzukuppeln. Gegebenenfalls ist nach dem Austausch von Batterien eine Synchronisation der Systemuhrzeit über das Tablet erforderlich.

Um die Batterien des Hybridzylinders zu wechseln, gehen Sie wie in der Montageanleitung angeführt, jedoch in umgekehrter Reihenfolge, vor.

- Setzen Sie das Zylinderwerkzeug vollständig auf die dafür vorgesehene Ausnehmung auf der Rückseite des Außenknaufs und schrauben Sie den Knauf und das Werkzeug gemeinsam (gegen den Uhrzeigersinn) herunter.
- Entfernen Sie das Zylinderwerkzeug und öffnen Sie die 3 Befestigungsschrauben mit einem Kreuzschraubendreher (PH1) auf der Rückseite des Außenknaufs.
- Nehmen Sie die Knaufscheibe ab.
- Öffnen Sie vorsichtig den Verschluss im Außenknauf, indem Sie diesen vorsichtig verschieben und dann aufklappen.
- Entnehmen Sie die beiden leeren Batterien CR2 und reinigen Sie die Batteriekontakte mit einem weichen, fusselfreien Tuch.
- Setzen Sie die beiden neuen Batterien lagerichtig in das Batteriefach ein und verschließen Sie dieses wieder.

Wenn der Batteriewechsel – die Stromunterbrechung – länger als eine Minute dauert, muss der Zylinder mit dem Tablet synchronisiert werden!

» Sollte der Batteriewechsel korrekt durchgeführt worden sein, erfolgt die Initialisierung und es ertönt die entsprechende Signalisierung. (Siehe Kapitel „Ereignissignalisierung", Signal 8 der Signalisierungstabelle).

» Setzen Sie die Knaufscheibe wieder auf und befestigen Sie sie mit den 3 Befestigungsschrauben.

» Setzen Sie das Zylinderwerkzeug auf der Rückseite des Außenknaufs vollständig auf und schrauben Sie den Knauf und das Werkzeug gemeinsam (im Uhrzeigersinn) auf den Zylinder, bis Sie einen Widerstand spüren.

» Drehen Sie den Zylinder anschließend in die entgegengesetzte Richtung (gegen den Uhrzeigersinn), bis Sie ein „Klick" hören.

» Nehmen Sie das Zylinderwerkzeug wieder ab.

» Nach erfolgreichem Batterietausch synchronisieren Sie die Komponente mit dem Tablet und der Xesar-Software. Dadurch wird der neue Batteriestatus in die Xesar-Software übertragen.

2.1.5 Hebelzylinder

- Batteriebetriebene Zutrittskomponente
- Einsatz im Außen- und Innenbereich
- Geeignet für Spinde, Vitrinen, verschiedene Behältnisse sowie Briefkästen.

Hebelzylinder (Symbolfoto)

❶ Optische Signalisierung
❷ Leseeinheit
❸ Stecker-Schnittstelle (EVVA-Logo)
Farbmarkierung (BLE oder 3-Zack) unter dem EVVA-Logo

Der Sensor der Leseeinheit befindet sich in der Kunststoffkappe des Zylinders, zwischen der Stecker-Schnittstelle und der optischen Signalisierung (LED).

Der Zylinder signalisiert Ereignisse sowohl akustisch als auch optisch.
Beachten Sie die Liste der unterschiedlichen akustischen und optischen Signale im Kapitel „Ereignissignalisierung".

Der Zylinder verfügt über eine Dauerfreigabe-Funktion. Beachten Sie dazu die Hinweise zur Dauerfreigabe-Funktion.

Funktionsprinzip

Der Zutritt erfolgt über eine elektronische Berechtigungsprüfung an der Außenseite des Hebelzylinders.

Auf der Innenseite befindet sich ein Hebel, der für die Verriegelung sorgt. Sowohl das Entriegeln, als auch das Verriegeln ist erst nach erfolgreicher Berechtigungsprüfung und durch manuelles Drehen des Hebelzylinders möglich. Der elektronische Knauf an der Identifikationsseite ist ohne Berechtigung nicht frei drehend.

Der Hebelzylinder steht in unterschiedlichen Bauformen und Konfigurationen zur Verfügung. Prüfen Sie, ob der ausgewählte Hebelzylinder Ihren Anforderungen entspricht.
Informationen zu weiteren Spezifikationen entnehmen Sie dem Datenblatt.

› **https://www.evva.com/at-de/service/downloads/**

Der Hebelzylinder besitzt eine optische und eine akustische Signalisierung. (Erläuterungen der verschiedenen Signale siehe Kapitel „Ereignissignalisierung".)

! Beachten Sie die mitgelieferte Montageanleitung.

Batteriewechsel

» Aktivieren Sie vor dem Batteriewechsel die Daueröffnung des Hebelzylinders, damit der Hebelzylinder eingekuppelt bleibt.

Der Betrieb des Zylinders ist nur mit Batterien der Type CR2 zulässig.

Eine Liste der empfohlenen Batteriemodelle erhalten Sie auf Anfrage bei Ihrem Fachhändler.

! Die Verwendung von Akkumulatoren (Akkus) ist unzulässig!

Lassen Sie die Batterien nur von geschultem Fachpersonal wechseln!

Wenn Signal „Batterie leer" angezeigt wird, müssen die Batterien umgehend gewechselt werden. (Wenn das Signal „Batterie leer" das erste Mal angezeigt wird, sind für einen Zeitraum von 4 Wochen maximal 1.000 Öffnungen möglich. Die Anzahl Öffnungen ist abhängig von der Raumtemperatur und kann entsprechend geringer sein.)

Der Hebelzylinder kann bei leeren Batterien nur mit dem Notstromgerät (optionales Zubehör) und einem Generalhauptschlüssel- oder Feuerwehr-Medium betätigt werden.

Tauschen Sie bei einem Batteriewechsel alle im Zylinder eingesetzten Batterien aus!

Verwenden Sie für die Montage bzw. Demontage des Knaufs (auch beim Batteriewechsel) das spezielle Montagewerkzeug für den Zylinder.

Wir empfehlen Ihnen, den Zylinder vor Entnahme der Batterien mittels eines berechtigten Zutrittsmediums einzukuppeln. Gegebenenfalls ist nach dem Austausch von Batterien eine Synchronisation der Systemuhrzeit über das Tablet erforderlich.

Um die Batterien des Hebelzylinders zu wechseln, gehen Sie wie in der Montageanleitung angeführt, jedoch in umgekehrter Reihenfolge, vor.

- Setzen Sie das Zylinderwerkzeug vollständig auf die dafür vorgesehene Ausnehmung auf der Rückseite des Außenknaufs und schrauben Sie den Knauf und das Werkzeug gemeinsam (gegen den Uhrzeigersinn) herunter.
- Entfernen Sie das Zylinderwerkzeug und öffnen Sie die 3 Befestigungsschrauben mit einem Kreuzschraubendreher (PH1) auf der Rückseite des Außenknaufs.
- Nehmen Sie die Knaufscheibe ab.
- Öffnen Sie vorsichtig den Verschluss im Außenknauf, indem Sie diesen vorsichtig verschieben und dann aufklappen.
- Entnehmen Sie die beiden leeren Batterien CR2 und reinigen Sie die Batteriekontakte mit einem weichen, fusselfreien Tuch.
- Setzen Sie die beiden neuen Batterien lagerichtig in das Batteriefach ein und verschließen Sie dieses wieder.

Wenn der Batteriewechsel – die Stromunterbrechung – länger als eine Minute dauert, muss der Zylinder mit dem Tablet synchronisiert werden!

» Sollte der Batteriewechsel korrekt durchgeführt worden sein, erfolgt die Initialisierung und es ertönt die entsprechende Signalisierung. (Siehe Kapitel „Ereignissignalisierung“, Signal 8 der Signalisierungstabelle).

» Setzen Sie die Knaufscheibe wieder auf und befestigen Sie sie mit den 3 Befestigungsschrauben.

» Setzen Sie das Zylinderwerkzeug auf der Rückseite des Außenknaufs vollständig auf und schrauben Sie den Knauf und das Werkzeug gemeinsam (im Uhrzeigersinn) auf den Zylinder, bis Sie einen Widerstand spüren.

» Drehen Sie den Hebelzylinder anschließend in die entgegengesetzte Richtung (gegen den Uhrzeigersinn), bis Sie ein „Klick“ hören.

» Nehmen Sie das Zylinderwerkzeug wieder ab.

» Nach erfolgreichem Batterietausch synchronisieren Sie die Komponente mit dem Tablet und der Xesar-Software. Dadurch wird der neue Batteriestatus in die Xesar-Software übertragen.

2.1.6 Hangschloss

- Batteriebetriebene Zutrittskomponente
- Einsatz im Außen- und Innenbereich
- Geeignet zur Absicherung von Schrankanlagen, Rollläden, Depots und Archivcontainern.
- Einfach und auch nachträglich in Anlagen integrierbar.

Beachten Sie die mitgelieferten Sicherheitstexte, die zusätzlich wichtige Informationen zu Montage, Gebrauch und Wartung der Zutrittskomponenten beinhalten.

› **https://www.evva.com/at-de/xesar/**

Hangschloss (Symbolfoto)

1. Optische Signalisierung
2. Leseeinheit
3. Stecker-Schnittstelle (EVVA-Logo)
   Farbmarkierung (BLE oder 3-Zack) unter dem EVVA-Logo

Der Sensor der Leseeinheit befindet sich in der Kunststoffkappe des Hangschlosses, zwischen der Stecker-Schnittstelle und der optischen Signalisierung (LED).

Das Hangschloss signalisiert Ereignisse sowohl akustisch als auch optisch.
Beachten Sie die Liste der unterschiedlichen akustischen und optischen Signale im Kapitel „Ereignissignalisierung".

Das Hangschloss verfügt über eine Dauerfreigabe-Funktion. Beachten Sie dazu die Hinweise zur Dauerfreigabe-Funktion.

Funktionsprinzip

Der elektronische Außenknauf des Hangschlosses ist standardmäßig ausgekuppelt; bei Betätigung des Knaufs bleibt die Sperrnase ausgekuppelt und der Knauf dreht, ohne die Sperrnase mitzunehmen.

Wird ein berechtigtes Identmedium an der Leseeinheit vorgehalten, wird der Knauf für 5 Sekunden mechatronisch eingekuppelt. Sowohl das Entriegeln, als auch das Verriegeln kann erst nach erfolgreicher Berechtigungsprüfung, durch manuelles Drehen am elektronischen Knauf des Hangschlosses, erfolgen.
Die Sperrnase des Hangschlosses wird bei der Betätigung des Knaufs mitgenommen.

Ereignisspeicher

Im Ereignisspeicher werden bis zu 1.000 Ereignisse gespeichert. Wenn der Ereignisspeicher voll ist, werden die Einträge der ältesten Ereignisse überschrieben.

Synchronisieren Sie die Ereignisse regelmäßig!
Damit verhindern Sie, dass protokollierte Ereignisse überschrieben werden.

Informationen zu weiteren Spezifikationen entnehmen Sie dem Datenblatt.

› **https://www.evva.com/at-de/xesar/**

Batteriewechsel

» Aktivieren Sie vor dem Batteriewechsel die Daueröffnung des Hangschlosses, damit das Hangschloss eingekuppelt bleibt.

Der Betrieb des Zylinders ist nur mit Batterien der Type CR2 zulässig.

Eine Liste der empfohlenen Batteriemodelle erhalten Sie auf Anfrage bei Ihrem Fachhändler.

Die Verwendung von Akkumulatoren (Akkus) ist unzulässig!

Lassen Sie die Batterien nur von geschultem Fachpersonal wechseln!

Wenn Signal „Batterie leer" angezeigt wird, müssen die Batterien umgehend gewechselt werden. (Wenn das Signal „Batterie leer" das erste Mal angezeigt wird, sind für einen Zeitraum von 4 Wochen maximal 1.000 Öffnungen möglich. Die Anzahl Öffnungen ist abhängig von der Raumtemperatur und kann entsprechend geringer sein.)

Das Hangschloss kann bei leeren Batterien nur mit dem Notstromgerät (optionales Zubehör) und einem Generalhauptschlüssel- oder Feuerwehr-Medium betätigt werden.

Tauschen Sie bei einem Batteriewechsel alle im Zylinder eingesetzten Batterien aus!

Verwenden Sie für die Montage bzw. Demontage des Knaufs (auch beim Batteriewechsel) das spezielle Montagewerkzeug für das Hangschloss.

Wir empfehlen Ihnen, den Zylinder vor Entnahme der Batterien mittels eines berechtigten Zutrittsmediums einzukuppeln. Gegebenenfalls ist nach dem Austausch von Batterien eine Synchronisation der Systemuhrzeit über das Tablet erforderlich.

Um die Batterien des Hangschlosses zu wechseln, gehen Sie wie in der Montageanleitung angeführt, jedoch in umgekehrter Reihenfolge, vor.

- Setzen Sie das Zylinderwerkzeug vollständig auf die dafür vorgesehene Ausnehmung auf der Rückseite des Knaufs und schrauben Sie den Knauf und das Werkzeug gemeinsam (gegen den Uhrzeigersinn) herunter.

- Entfernen Sie das Zylinderwerkzeug und öffnen Sie die 3 Befestigungsschrauben mit einem Kreuzschraubendreher (PH1) auf der Rückseite des Knaufs.

- Nehmen Sie die Knaufscheibe ab.

- Öffnen Sie vorsichtig den Verschluss im Knauf, indem Sie diesen vorsichtig verschieben und dann aufklappen.

- Entnehmen Sie die beiden leeren Batterien CR2 und reinigen Sie die Batteriekontakte mit einem weichen, fusselfreien Tuch.

- Setzen Sie die beiden neuen Batterien lagerichtig in das Batteriefach ein und verschließen Sie dieses wieder.

Wenn der Batteriewechsel – die Stromunterbrechung – länger als eine Minute dauert, muss der Zylinder mit dem Tablet synchronisiert werden!

- Sollte der Batteriewechsel korrekt durchgeführt worden sein, erfolgt die Initialisierung und es ertönt die entsprechende Signalisierung. (Siehe Kapitel „Ereignissignalisierung", Signal 8 der Signalisierungstabelle).

- Setzen Sie die Knaufscheibe wieder auf und befestigen Sie sie mit den 3 Befestigungsschrauben.

- Setzen Sie das Zylinderwerkzeug auf der Rückseite des Knaufs vollständig auf und schrauben Sie den Knauf und das Werkzeug gemeinsam (im Uhrzeigersinn) auf den Zylinder, bis Sie einen Widerstand spüren.

- Drehen Sie den Zylinder anschließend in die entgegengesetzte Richtung (gegen den Uhrzeigersinn), bis Sie ein „Klick" hören.

- Nehmen Sie das Zylinderwerkzeug wieder ab.

- Nach erfolgreichem Batterietausch synchronisieren Sie die Komponente mit dem Tablet und der Xesar-Software. Dadurch wird der neue Batteriestatus in die Xesar-Software übertragen.

2.1.7 Zylinderwerkzeug

Der Zylinder bietet zum Schutz gegen Manipulation einen speziellen Öffnungsmechanismus. Für die Montage, Demontage und Batteriewechsel benötigen Sie ein spezielles Zylinderwerkzeug.

Zylinderwerkzeug (Symbolfoto)

Das Zylinderwerkzeug ist im Lieferumfang des Zylinders nicht enthalten.

Option Das Zylinderwerkzeug ist optional erhältlich:
Produktcode: E.ZU.PZ.ZW.V2

Wenn der Batteriewechsel – die Stromunterbrechung – länger als eine Minute dauert, muss der Zylinder mit dem Tablet synchronisiert werden!

2.1.8 Wandleser

- Einsatz im Außen- und Innenbereich, Unter- oder Aufputz
- Geeignet für sicherheitsrelevante Bereiche
- Der Wandleser wird mit der Steuereinheit mittels Anschlusskabel (CAT5-Kabel, max. 100 m, Loop max. = 2 Ohm) verbunden und von dieser stromversorgt.
- Über die mit dem Wandleser verbundene Steuereinheit können elektronische Verschlusselemente, wie z. B. Motorzylinder, Schwenktüren oder Schiebetüren angesteuert werden.

Beachten Sie die mitgelieferten Sicherheitstexte, die zusätzlich wichtige Informationen zu Montage, Gebrauch und Wartung der Zutrittskomponenten beinhalten.

› **https://www.evva.com/at-de/xesar/**

Verwenden Sie in Außen- oder Nassbereichen sowie bei Unterputzmontage die dafür vorgesehene Dichtung (liegt dem Produkt bei).

Wandleser (Symbolfoto)

1. Optische Signalisierung
2. Leseeinheit und ON/OFF-Statusleuchte
3. Stecker-Schnittstelle (EVVA-Logo)
   Farbmarkierung (BLE oder 3-Zack) unter dem EVVA-Logo

Der Wandleser kann nur in Verbindung mit einer Steuereinheit verwendet werden.

Die Stecker-Schnittstelle dient ausschließlich der Synchronisation mit dem Tablet. Der Wandleser kann NICHT mit dem optional erhältlichen Notstromgerät versorgt werden.

Der Sensor der Leseeinheit befindet sich hinter der Glasplatte des Wandlesers, zwischen der Stecker-Schnittstelle und der optischen Signalisierung (LED). Die ON/OFF-Statusleuchte leuchtet im laufenden Betrieb durchgehend und erleichtert so die Lokalisierung des Lesebereichs in dunkler Umgebung.

Der Wandleser signalisiert Ereignisse sowohl akustisch als auch optisch.
Beachten Sie die Liste der unterschiedlichen akustischen und optischen Signale im Kapitel „Ereignissignalisierung".

Der Wandleser verfügt über eine Dauerfreigabe-Funktion. Beachten Sie dazu die Hinweise zur Dauerfreigabe-Funktion.

Funktionsprinzip

Wird ein Zutrittsmedium an der Leseeinheit vorgehalten, wird dieses Zutrittsmedium von der Steuereinheit, die mit dem Wandleser verbunden ist, geprüft. Bei Berechtigung wird – abhängig von der Jumperstellung – und der Konfiguration, das jeweils angesprochene Relais der Steuereinheit geschaltet.
(Beachten Sie den Deckelplan, JP2 in der Steuereinheit.)

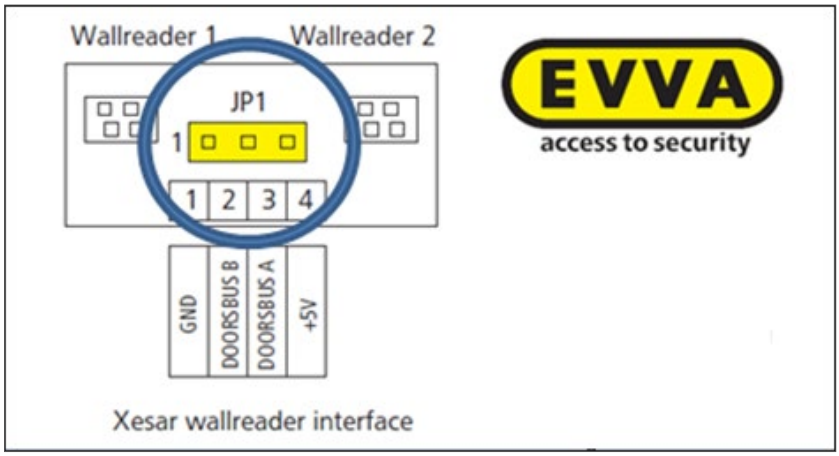
Ereignisspeicher

Im Ereignisspeicher der Steuereinheit werden bis zu 1.000 Ereignisse gespeichert. Wenn der Ereignisspeicher voll ist, werden die Einträge der ältesten Ereignisse überschrieben.

Synchronisieren Sie die Ereignisse regelmäßig!
Damit verhindern Sie, dass protokollierte Ereignisse überschrieben werden.

Anschlussprint

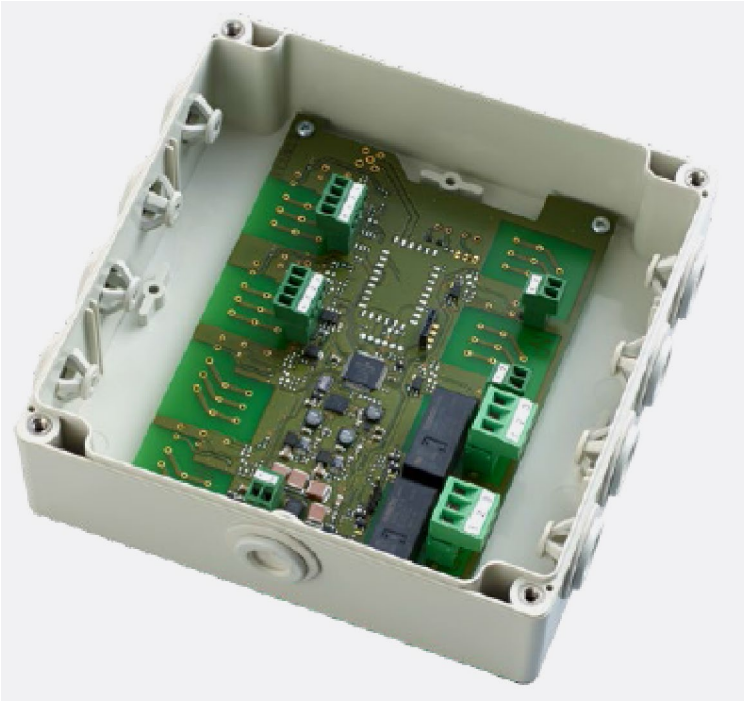
Der Wandleser wird mittels Anschlussprint an die Verbindungsleitung der Steuereinheit angeschlossen.



Anschlussprint für Xesar-Wandleser (Symbolfoto)

Beachten Sie die Anweisungen zur Jumperstellung des Jumpers JP1 in der Montageanleitung, um eine Fehlfunktion zu vermeiden.

Offline-Steuereinheit



Steuereinheit (Symbolfoto)

Die Wandleser-Offline-Steuereinheit kann ausschließlich in Verbindung mit dem Wandleser betrieben werden. Die Wartung der Offline-Wandleser erfolgt mit dem Tablet. Der Datenaustausch mit der Software erfolgt mittels Tablet oder über XVN mit den Zutrittsmedien. Es können bis zu 2 Wandleser angeschlossen werden. Die mit dem Wandleser verbundene Steuereinheit muss manipulationsgeschützt im Innenbereich montiert werden.

Sobald die Steuereinheit mindestens 6 Stunden mit dem Stromnetz verbunden war, wird gewährleistet, dass die Uhrzeit im Fall einer Netzunterbrechung für einen Zeitraum von 72 Stunden erhalten bleibt.

An die Steuereinheit kann ein externes Freigabeelement (Austrittstaster) angeschlossen werden. Bei Betätigung des Tasters öffnet sich die Tür und die Öffnung wird im Ereignisprotokoll protokolliert.

Die Steuereinheit wird mittels Netzteil stromversorgt und verfügt bei Stromausfall über eine Datenpufferung von max. 72 Stunden, wenn sie vorher mindestens 6 Stunden in Betrieb war.

Online-Steuereinheit

Die Wandleser-Online-Steuereinheit kann ausschließlich in Verbindung mit dem Wandleser betrieben werden. Je Online-Steuereinheit kann maximal 1 Wandleser angeschlossen werden. Die mit dem Wandleser verbundene Online-Steuereinheit muss im manipulationsgeschützten Innenbereich montiert werden.

Weitere Informationen zum Online-Wandleser erhalten Sie im Kapitel „Online-Wandleser".

An die Steuereinheit kann ein externes Freigabeelement (Austrittstaster) angeschlossen werden. Bei Betätigung des Tasters öffnet sich die Tür und die Öffnung wird im Ereignisprotokoll protokolliert.

Zur Türüberwachung kann ein Türkontakt an die Steuereinheit angeschlossen werden. In der Xesar-Software werden die Zeitpunkte der Tür-Öffnungen und -Schließungen protokolliert und der aktuelle Türzustand (offen/geschlossen) angezeigt.

Über die Xesar-Software kann die Online-Tür aus der Ferne geöffnet und auch in den Office-Mode geschaltet werden.

Die Online-Steuereinheit ist über den Ethernet Adapter via LAN mit dem Anlagenrechner verbunden. Unterbricht die LAN-Verbindung, agiert der Wandleser wie ein Offline-Wandleser. Die Online-Steuereinheit wird mit einem Netzteil stromversorgt und verfügt bei Stromausfall über eine Datenpufferung von max. 72 Stunden, wenn sie vorher mindestens 6 Stunden in Betrieb war.

Betreiben Sie die Wandleser-Steuereinheiten über eine unabhängige Stromversorgung und sorgen Sie zusätzlich für eine unterbrechungsfreie Stromversorgung mit 12 Volt. Damit wird der Ausfall der Anlage verhindert und der Zutritt bleibt aufrecht.

Netzteil für Steuereinheit

Das Netzteil für die Steuereinheit ist im Lieferumfang nicht enthalten.

Option Zur Steuereinheit ist optional ein Netzteil erhältlich:
Produktcode: E.ZU.WL.NT.V2

2.2 Montage der Zutrittskomponenten

Lassen Sie die Zutrittskomponenten nur von geschultem Fachpersonal installieren.

Beachten Sie, dass Sie die Reihenfolge der beschriebenen Installationsschritte einhalten, um Fehlfunktion zu vermeiden.

Beachten Sie die mitgelieferten Sicherheitstexte, die zusätzlich wichtige Informationen zu Montage, Gebrauch und Wartung der Zutrittskomponenten beinhalten.

❯ **https://www.evva.com/at-de/xesar/**

In den Montageanleitungen bzw. auf den Verpackungen befinden sich QR-Codes, die Sie direkt zur jeweiligen Videosequenz des Montagevideos bzw. zur Montageanleitung führen.

Als Unterstützung zum Einbau der Zutrittskomponenten stellt EVVA unter anderem folgende Hilfsmittel zur Verfügung:

- Sprachneutrale Montageanleitung
  Die sprachneutrale Montageanleitung wird der entsprechenden Systemkomponente beigelegt. Zusätzlich werden sie auf der Homepage im Download-Bereich angeboten.

  ❯ **https://www.evva.com/at-de/xesar/**

- Produktabhängige Montagevideos
  Für komplexere Montageschritte stehen spezielle Videos mit Vorführungen bereit.

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

- Sprachneutrale Bohrschablone
  Die sprachneutrale Bohrschablone wird der entsprechenden Systemkomponente, die ein oder mehrere Bohrlöcher erfordert, beigelegt. Zusätzlich wird sie auf der Homepage im Download-Bereich angeboten.

  ❯ **https://www.evva.com/at-de/xesar/**

Optional gibt es für die Montage der Beschläge und Drücker eine Bohrschablone aus Metall.

Ein verstellbarer Anschlag sichert die korrekte Ausrichtung der Bohrungen und ermöglicht eine an die Anforderungen der jeweiligen Türsituation angepasste Einstellung. Die Bohrbuchsen sind aus Hartmetall, damit auch bei intensivem Gebrauch eine lange Lebensdauer garantiert ist.

Option Hochwertige Bohrschablone aus Metall:
Produktcode: E.ZU.BE.BS.V1

2.3 Ereignissignalisierung

Signal-nummer	Ereignis	Optisches Signal*	Akustisches Signal**	Hinweis
Signal 1	Öffnungsversuch mit berechtigtem Medium	●●●●●	mmmmm	Wenn mehrere Karten im Feld sind, erfolgt die Signalisierung erst nach der letzten gelesenen Karte (Ja / Nein / keine EVVA-Karte dabei)
Signal 2	Ende Freigabe	●●●●●	ttttt	
Signal 3	Abgewiesenes Medium	●●-●●-●●-●●	hh-hh-hh-hh	
Signal 4	Öffnungsversuch mit berechtigtem Medium bei aktiviertem Office-Mode (Dauerfreigabe)	●●●●--●●●●	tttt--hhhh	
Signal 5	Office-Mode (Dauerfreigabe) Start	●●●●--●●●●	tttt--hhhh	
Signal 6	Office-Mode (Dauerfreigabe) Ende	●●●●--●●●●	hhhh--tttt	
Signal 7	Öffnungsversuch mit berechtigtem Medium, Signalisierung Batterie leer	●●--●●--●●--	h----h----h----	
Signal 8	Batterie eingelegt bzw. Reboot der Komponente	●●--●●--●●	tt—mm—hh	Batterie-Ladezustandsanzeige; wird ggf. nach dem Batteriewechsel angezeigt
Signal 9	Medium ohne EVVA Segmentierung; Medium defekt, andere Anlage			Keine Signalisierung
Signal 10	Hardware defekt	●---●---●---●	mmm---mmm---	
Signal 12	Kommunikation erfolgreich	●●●●●	hhhhh	
Signal 13	Kommunikation nicht erfolgreich	●●●●●	ttttt	
Signal 14	Medium berechtigt Offline	●●-●●-●●	mm-mm-mm	
Signal 15	Abgewiesenes Medium Offline	●●-●●-●●	mm-mm-mm	
Signal 16	Online Operation fehlgeschlagen	●●-●●-●●		

Signal-nummer	Ereignis	Optisches Signal*	Akustisches Signal**	Hinweis
Signalisierung für G2.1-Komponenten:				
Signal 17	BLE aktivieren (Medium 2× anhalten)	1.: 🟡🟡 2.: 🟡🟡--🔵🔵🔵🔵--🟢🟢🟢🟢	tttt--hhhh	BLE On
Signal 18	BLE deaktivieren (Medium 2× anhalten)	1.: 🟡🟡 2.: 🟡🟡--🔵🔵🔵🔵--🔴🔴🔴🔴	hhhh--tttt	BLE Off
Signal 19	BLE Komponente identifizieren	🟡🟡---🟢🟢---🟢🟢--🟡🟡---🟡🟡--- 🟢🟢---🟢🟢---🟡🟡	hh---mm---mm---hh---hh---mm---mm---hh	wird am Tablet ausgelöst

* Optische Signale (LED): 🟡 = Rot 🔴 und Grün 🟢 gleichzeitig
** Akustische Signale: h = hoher Ton, m = mittlerer Ton, t = tiefer Ton
Jedes Signal entspricht einer Dauer von 50 ms.
Pausen werden mit – gekennzeichnet.

2.4 Codierstation

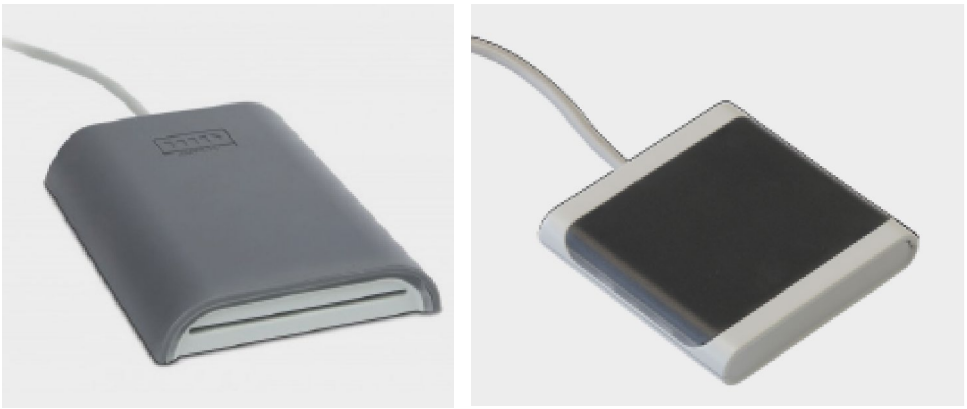
Die Codierstation ist das Lese-/Schreibgerät für alle kontaktlosen Identmedien sowie für die kontaktbehaftete Admin-Karte, die zu den Systemkarten zählt (siehe Kapitel „Admin-Karte").

Die Mini-Codierstation kann nicht für den Betrieb der Admin-Karte verwendet werden.

Für die Admin-Karte steht ein eigener Karteneinschub-Slot am vorderen Ende der Codierstation zur Verfügung.

» Verbinden Sie die Codierstation mit der USB-Schnittstelle Ihres Computers.

Wenn Ihr Betriebssystem die Codierstation nicht automatisch erkennt,
» installieren Sie den entsprechenden Treiber.



Codierstation und Mini-Codierstation (Symbolfotos)

Der Treiber für die Codierstation kann heruntergeladen werden:

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

Informationen zu weiteren Spezifikationen entnehmen Sie dem Datenblatt.

2.5 Tablet

Das Tablet dient zur Synchronisation und Übertragung von Informationen zwischen der Xesar-Software und den Zutrittskomponenten.

Tablet (Symbolfoto)

Laden Sie Ihr Xesar-Tablet vor der ersten Verwendung vollständig auf.

Für das Tablet wird eine eigene Bedienungsanleitung des Herstellers mitgeliefert. Diese befindet sich in der Verpackung des Produkts.

Installieren Sie keine zusätzlichen Applikationen, damit EVVA die Produktsicherheit und Funktionsfähigkeit gewährleisten kann.

Installieren Sie keine Betriebssystemupdates.

Ab der Xesar-Version 3.1 können Zutrittskomponenten der Generation G2.1 mit dem Tablet Ares BLE 4.2 zusätzlich zur kabelgebundenen Schnittstelle auch über die drahtlose BLE-Schnittstelle synchronisiert und gewartet werden.
Dazu muss am Tablet und an den Komponenten die BLE Funktion aktiviert sein. Alle Synchronisations- und Wartungsaufgaben, wie Konfigurationsänderungen, Ereignisdaten-Synchronisation oder Firmware-Updates können an allen in Reichweite befindlichen Zutrittskomponenten nach erfolgreicher Verbindung durchgeführt werden. (Siehe dazu auch Kapitel „Wartungsaufgaben mit Tablet durchführen“.)

Sie können auch das spezielle Verbindungskabel von EVVA verwenden, um Ihre Zutrittskomponenten mit dem Tablet zu verbinden.

Das spezielle Verbindungskabel ist am EVVA-Logo, das sich auf dem USB-Stecker befindet, zu erkennen. Jede Zutrittskomponente verfügt über eine eingebaute Stecker-Schnittstelle für die Synchronisation mit der Xesar-Software. Die Stecker-Schnittstelle der Zutrittskomponente befindet sich an der Vorderseite hinter dem EVVA-Logo (siehe Kapitel „Xesar-Zutrittskomponenten").

Synchronisieren Sie regelmäßig die Daten mit Ihren Zutrittskomponenten.

Im Ereignisspeicher jeder Zutrittskomponente werden bis zu 1.000 Ereignisse gespeichert. Wenn der Ereignisspeicher voll ist, werden die Einträge der ältesten Ereignisse überschrieben.
Durch regelmäßige Synchronisation verhindern Sie, dass protokollierte Ereignisse überschrieben werden.

Synchronisieren Sie Ihre Zutrittskomponenten mindestens einmal jährlich, um die Uhrzeit der Zutrittskomponenten synchron zu halten.

Wenn Sie Online-Komponenten verwenden, werden die Daten über XVN aktuell gehalten.

Das Tablet darf nicht für die Notstromversorgung der batteriebetriebenen Zutrittskomponenten verwendet werden.

Schließen Sie die Stecker-Abdeckung nach Gebrauch wieder, um die Stecker-Schnittstelle vor Staub und Feuchtigkeit zu schützen.

Verwenden Sie KEINE spitzen Gegenstände, um die Stecker-Abdeckung zu öffnen.

Informationen zu weiteren Spezifikationen entnehmen Sie dem jeweiligen Datenblatt.

https://www.evva.com/at-de/xesar/

Funktionsprinzip

Bei jeder Synchronisation des Tablets mit der Xesar-Software werden alle Wartungsaufgaben und andere Aufgaben für die jeweilige Zutrittskomponente auf das Tablet geladen und protokolliert.

Verbinden Sie das Tablet mittels drahtloser BLE-Schnittstelle oder dem Verbindungskabel mit den Zutrittskomponenten. Der Datenaustausch wird mittels der Xesar-Wartungsapp (Applikation) durchgeführt.

Xesar-Wartungsapp

Die Xesar-Wartungsapp ist auf dem Tablet vorinstalliert.

Folgende Aktionen sind mit der Xesar-Wartungsapp möglich:

- Zutrittskomponenten zur Anlage hinzufügen
- Geänderte Türparameter bei Zutrittskomponenten synchronisieren
- Blacklist auf Zutrittskomponenten übertragen
- Aktuellen Batteriestatus prüfen
- Aktuelle Firmware-Version abfragen
- Firmware-Update durchführen
  Die Zutrittskomponente im Batteriebetrieb wird während des Firmware-Updates durch das Tablet mit Energie versorgt. Es können auch Firmware-Updates im Baustellenmodus mit höheren Firmwareständen, als in der Anlage vorhanden sind, durchgeführt werden.
- Ereignisse von Zutrittskomponenten auf Xesar-Tablet übertragen
- Zutrittskomponente in Baustellenmodus zurücksetzen
- Die Uhrzeit der Zutrittskomponente wird bei der Kommunikation mit dem Tablet automatisch synchronisiert.
- BLE-Zutrittskomponenten mittels Identifikationsfunktion lokalisieren

2.6 Notstromgerät

Das Notstromgerät versorgt die Zutrittskomponente bei Bedarf mit Strom. Dadurch kann die Zutrittskomponente auch bei leeren Batterien bedient werden.

Sie benötigen zur Öffnung der notstromversorgten Zutrittskomponente ein Zutrittsmedium mit Generalhauptschlüssel- oder Feuerwehr-Berechtigung, da bei zu langer Stromunterbrechung die Uhrzeit verloren geht.

Notstromgerät (Symbolfoto)

» Schließen Sie das Verbindungskabel des Notstromgeräts an der Stecker-Schnittstelle der entsprechenden Zutrittskomponente an.

» Schalten Sie das Notstromgerät ein.

Eine weitere Interaktion am Notstromgerät selbst ist nicht erforderlich. Zur Bedienung der Zutrittskomponente wird ein Medium mit gültiger Generalhauptschlüssel- oder Feuerwehr-Berechtigung benötigt.

» Nach der Notstromöffnung nehmen Sie sofort einen Batteriewechsel an der Zutrittskomponente vor.
Aktualisieren Sie die Zutrittskomponente mit dem Tablet. Damit wird der Zutritt mit allen berechtigten Identmedien wieder möglich.

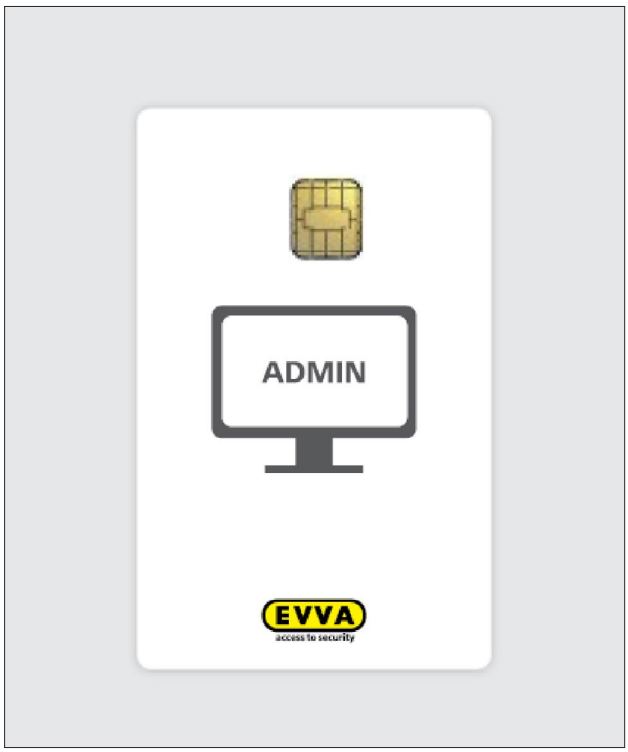
Die in der Zutrittskomponente eingebaute Stecker-Schnittstelle wird in Zusammenhang mit dem Notstromgerät nur für die Notstromversorgung benötigt.

Das Notstromgerät ist optional erhältlich.

Option Zur Steuereinheit ist optional ein Netzteil erhältlich:
Produktcode: E.ZU.NG.V1

2.7 Admin-Karte

Die Admin-Karte ist eine kontaktbehaftete, elektronische Chipkarte im Standardformat. Die Admin-Karte ermöglicht den Zugriff auf die Xesar-Software und identifiziert die Anlage eindeutig.



Admin-Karte (Symbolfoto)

Auf der Admin-Karte werden die für Berechtigungsänderungen erworbenen KeyCredits gespeichert. (Das gilt nicht für KeyCredit Xesar Lifetime.)

Systemänderungen oder Aufladen von KeyCredits ist nur möglich, wenn sich eine gültige Admin-Karte in der Codierstation befindet. Die Admin-Karte ist nur für Lizenzoperationen notwendig.

Die Admin-Karte ist nicht übertragbar und kann daher nicht für andere Anlagen genutzt werden.

Bei Verlust oder Defekt kann die Admin-Karte ausgetauscht werden.

2.8 Zutrittsmedien

Zutrittsmedien (Karten, Schlüsselanhänger, Kombischlüssel) dienen zum Öffnen von Türen bzw. zum Transport von anlagenspezifischen Sicherheitsdaten zwischen Zutrittskomponenten und der Verwaltungssoftware über das virtuelle Netzwerk XVN (Xesar Virtuelles Netzwerk).

Zutrittsmedien im Überblick

Zutrittsmedien sind berührungslose RFID[1]-Chips, die auf MIFARE[2] DESFire EV1 mit einer Gesamtspeichergröße von 4 kB basieren.

- Mit Zutrittsmedien werden die Zutrittskomponenten geöffnet.
  Die Anlage darf sich dazu nicht im Baustellenmodus befinden. Im Baustellenmodus wurde die Zutrittskomponente noch keiner Anlage elektronisch zugewiesen. Jede Zutrittskomponente befindet sich im Auslieferungszustand im Baustellenmodus. Zutrittskomponenten im Baustellenmodus können nur mit speziellen Baustellenmedien geöffnet werden.

- Mit der Codierstation werden Zutrittsmedien programmiert.
  Legen Sie dazu das Zutrittsmedium auf die betriebsbereite Codierstation und führen Sie die entsprechenden Interaktionen in der Xesar-Software durch.

Legen Sie immer nur ein Zutrittsmedium auf die Codierstation. Damit vermeiden Sie fehlerhafte Beschreibung der Zutrittsmedien.

Halten Sie die Codierstation frei von metallischen Gegenständen, damit die Lesequalität nicht beeinträchtigt wird.

1 RFID – radio-frequency identification
2 MIFARE – Mikron Fare Collection System (kontaktlose Chipkartentechnik)

Informationen zu weiteren Spezifikationen entnehmen Sie dem Datenblatt.

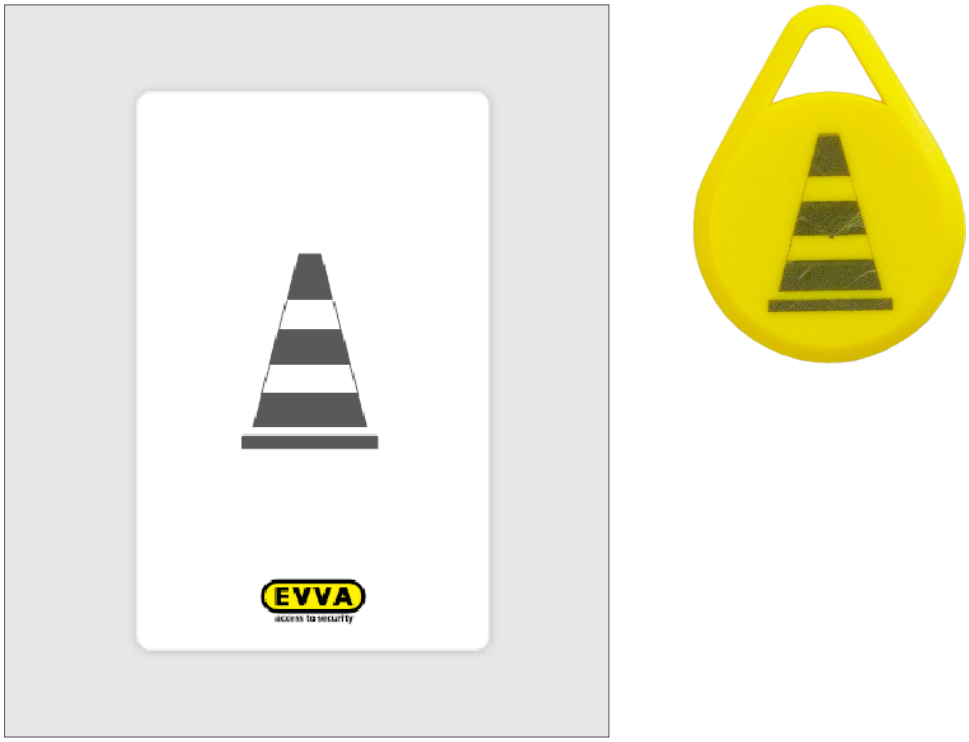
https://www.evva.com/at-de/xesar/

Anzahl der Berechtigungen pro Zutrittsmedium: max. 96 Türbereiche (unabhängig von der Anzahl der zum Bereich gehörenden Einbauorte).
Zusätzlich 32 Einbauorte.

2.9 Baustellenmedien

Baustellenmedien gibt es in Form von Karten und Schlüsselanhänger. Damit können Zutrittskomponenten im Baustellenmodus geöffnet werden. (Im Baustellenmodus wurde die Zutrittskomponente noch keiner Anlage elektronisch zugewiesen. Jede Zutrittskomponente befindet sich im Auslieferungszustand im Baustellenmodus.)

Zusätzlich ist den Baustellenmedien die Funktion einer manuellen Dauerfreigabe möglich (siehe Kapitel „Zeitprofile“).



Baustellenmedien (Symbolfotos)

Die Baustellen-Karte ist eine berührungslose Chipkarte, die mit einem RFID-Chip, der auf MIFARE DESFire EV1 basiert, ausgestattet ist.

Ihre Anlage kann im Baustellenmodus mit jedem Baustellenmedium bedient werden! Legen Sie daher sobald als möglich eine Anlage an und fügen Sie Ihre Zutrittskomponenten hinzu.

Für eine effiziente Inbetriebnahme der Anlage legen Sie zuerst Berechtigungsprofile sowie zugehörige Bereiche und Zeitprofile an.
Konfigurieren Sie diese dann gleichzeitig mit dem Hinzufügen der Zutrittskomponenten. (Siehe Kapitel „Inbetriebnahme der Xesar-Software“.)

2.10 Bluetooth-On/Off-Medien

Bluetooth-On/Off-Medien gibt es in Form von Karten und Schlüsselanhänger. Durch zweimaliges Anhalten der Bluetooth-On/Off-Karte an der Zutrittskomponente kann die Bluetooth-Sendefunktion der Zutrittskomponente aktiviert oder deaktiviert werden. Die Zutrittskomponente muss sich dabei im Baustellenmodus befinden. Der jeweilige Sendestatus wird mit optischen und akustischen Signalen angezeigt. (Siehe dazu auch Kapitel „Ereignissignalisierung“.)

Die Bluetooth-Sendefunktion kann aus folgenden Gründen deaktiviert werden:

- Verwendung in Xesar 2.2- oder Xesar 3.0-Anlagen
- Verlängerung der Batterielebensdauer
- Verwendung in funktechnisch sensiblen Bereichen

In diesen Fällen erfolgt die Wartung der Zutrittskomponenten mittels USB-Kabel.

Wenn BLE-Komponenten aus einer Anlage ausgebaut oder zurückgesetzt werden, bleiben sie im zuletzt eingestellten BLE-Sendemodus.

Bluetooth-On/Off-Medien (Symbolfotos)

Diese Funktion ist nur bei BLE-fähigen G2.1-Zutrittskomponenten möglich.

3 Projekt-Checkliste und System-anforderungen

3.1 Vorwort

Dieses Dokument dient zur Unterstützung der Projektierung von Xesar 3.1-Anlagen. Es umfasst 3 Teile.

Teil 1 ist die Projekt-Checkliste, in der wichtige Anforderungen und Daten der neuen Xesar 3.1-Anlage systematisch abgefragt und für die weitere Planung dokumentiert werden.

Teil 2 beschreibt die technischen Systemanforderungen für eine Xesar 3.1-Anlage auf PC und für eine Xesar 3.1-Anlage auf Server.

Teil 3 beinhaltet als Anhang detaillierte technische Informationen zur Verteilsicht und System-Kommunikation einer Xesar 3.1-Anlage.

Verwenden Sie dieses Dokument als Unterstützung zur Planung Ihrer Xesar 3.1-Anlage.

Zur Abklärung der notwendigen IT-Infrastruktur gemäß den Xesar 3.1-Systemanforderungen wenden Sie sich bitte an Ihren IT-Administrator.

Bei Fragen zur Projekt-Checkliste oder den Xesar 3.1-Systemanforderungen wenden Sie sich bitte an Ihren EVVA-Partner oder an das Technische Büro von EVVA.

4 Projekt-Checkliste

Projekttitel:

Kontaktpersonen:

Projekt:

Telefon:

E-Mail:

IT:

Telefon:

E-Mail:

Anlagenadresse:

Gewünschter Fertigstellungstermin:

4.1 Anlagenanforderungen – Infrastruktur

Anlagenart
Für eine detaillierte Beschreibung der Systemanforderungen siehe
- Xesar 3.1 Einplatz-Anlage
- Xesar 3.1 Mehrplatz-Anlage

Einplatz: Windows 10 PRO PC Type:

Mehrplatz: Server Installation:
- Admin-PC: Windows 10 PRO PC, Type:
- Client-PC: Type:
- Server vorhanden? Ja / Nein

  Wenn **Ja**:
  Server Hardware:

  Server Betriebssystem:

  Hypervisor z.B. VMware:

  (Siehe auch Kapitel „Systemanforderungen für den Betrieb eines Xesar 3.1-Servers.)

  Wird der Server nur für Xesar verwendet? Ja / Nein
  Wenn **Nein**:
  Welche anderen Anwendungen, außer Xesar, laufen noch am Server?

Anlagentyp

Neuanlage

Upgrade von Bestandsanlage Xesar Version: X2.2 X3.0

Vor einem Upgrade auf Xesar 3.1 muss die Bestandsanlage auf die Version Xesar 2.2 V2.2.38.43 aktualisiert werden und die letztgültigen Xesar 2.2-Firmwarestände eingespielt sein! Weiters müssen alle offenen Wartungsaufgaben durchgeführt werden.

Ist die Konfiguration „2 Wandleser – 1 Steuereinheit" bei der Bestandsanlage vorhanden?

Ja Nein

Netzwerk

WLAN vorhanden (Voraussetzung für Xesar-Tablet Synchronisation)

Netzwerk-Name: Passwort:

LAN vorhanden

Ports sind konfigurierbar

(Siehe auch Kapitel „Systemanforderungen für das Netzwerk".)

Backup und Datensicherung sind definiert und lokal vorhanden (die Verantwortung zur Datensicherung liegt beim Betreiber/Benutzer).

Schnittstellenanforderungen

Datentransfer oder Steuerung vom Drittsystem gefordert

Beschreibung der Schnittstellenanforderung:

Schnittstellenspezifikation des Drittsystems ist vorhanden

Beschreibung:

4.2 Anlagenkonfiguration

Gewünschtes Bezahlmodell
(12 und 36 Monate KeyCredits sind auf Xesar 3.1 nicht übertragbar)

Stück KeyCredits (10/50/100) KeyCredit Xesar Lifetime

Anzahl der Arbeitsplätze

Anzahl der Arbeitsplätze mit Codierstation:
(mit Anlagen- und Zutrittsmedienverwaltung, PC-Administratorenrechte notwendig)

Anzahl der Arbeitsplätze ohne Codierstation: (Nur Anlagenverwaltung)

Anzahl der Xesar-Tablets: (für Wartungs- und Konfigurationsaufgaben)

Geplante Anzahl der Türen (Einbauorte) im Endausbau Stk.

Elektronische Zutrittskomponenten

Beschlag: Stk.

Drücker: Stk.

Online-Wandleser: Stk.

Offline-Wandleser: Stk.

Zylinder: Stk.

Weitere Komponenten: Stk.

Hybridanlage (Elektronische Komponenten und mechanische Zylinder)

EVVA Anlagennummer:

Anzahl der mechanischen Zylinder: Stk.

Geplante Anzahl der Zutrittsmedien Stk.

Karten: Stk.

Schlüsselanhänger: Stk.

Kombischlüssel: Stk.

Bestehende mechanische Schließanlagen
EVVA Anlagennummer

4.3 Anlagenprojektierung

Anlage mit mehreren verteilten Standorten (Mehrplatz-Anlage):

Eigen- oder Fremdverwaltung der Anlage (z.B. EVVA Partner, IT-Dienstleister):

Serverstandort:

Netzwerk der Zutrittsanlage:

Zukünftige Anlagenerweiterung geplant:

Projektierungsunterstützung gewünscht:

Häufigkeit an Zutrittsberechtigungs-Änderungen:

Schließplanerstellung & Berechtigungsvergabe:

Prüfung kundeneigener Zutrittsmedien (Fremdmediensegmentierung):

Brandschutzvorschriften berücksichtigt:

Fluchtwegvorschriften berücksichtigt:

Datenschutzanforderungen (z.B. DSGVO) berücksichtigt:

Arbeitnehmerschutz berücksichtigt:

Wartung & Support (Wartungsvertrag):

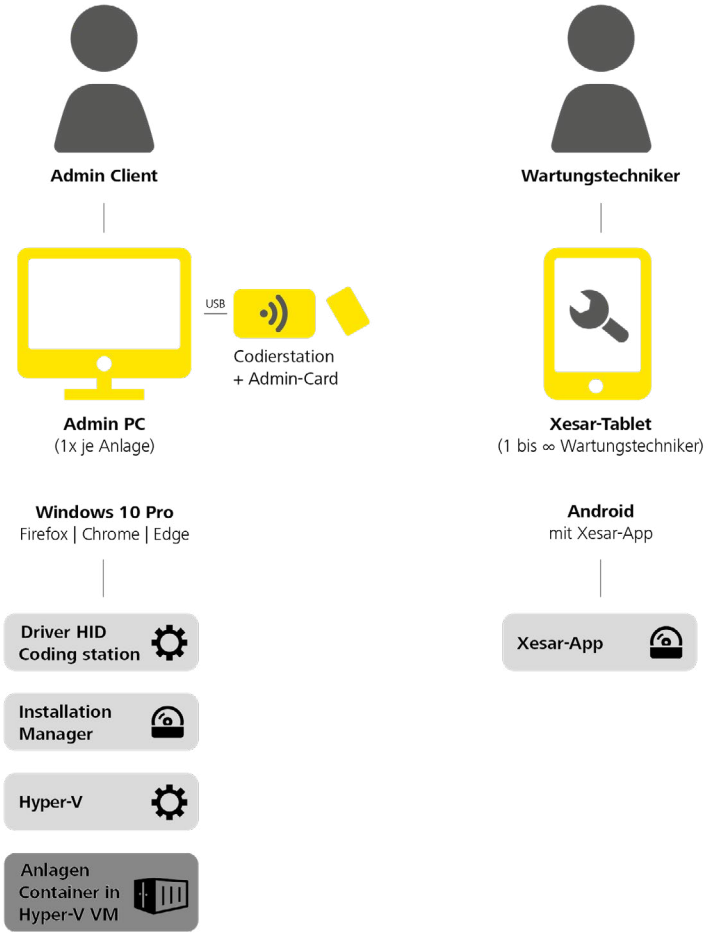
Sonstige Vereinbarungen:

5 Systemanforderungen für Einplatz- und Mehrplatz-Anlagen

Xesar kann sowohl als Einplatz-Anlage, als auch als Mehrplatz-Anlage betrieben werden. Nachstehend die Systemanforderungen.

5.1 Xesar 3.1-Einplatz-Anlage

Der Betrieb als Xesar-Anlage auf PC wird nicht für einen 24/7 Dauerbetrieb und den Einsatz mit Online-Komponenten (z. B. Online-Wandleser) empfohlen. Ist der PC für die Xesar-Anlage auf PC nicht in Betrieb, ist der Online-Wandleser im Offline-Modus und Zutrittsmedien werden nicht aktualisiert. Der Betrieb der Zutrittsanlage ist weiterhin gewährleistet.



Für den Betrieb einer Xesar-Anlage auf PC müssen folgende Mindestanforderungen erfüllt sein:

- x86-64 kompatibler Prozessor (CPU); mindestens Quad-Core ≥ 1,5-2,3 GHz
- Hardware-Unterstützung für Virtualisierung
- Arbeitsspeicher (RAM): ≥ 16 GB (mit OS); 4 GB freier Speicher für die Installation
- Festplattenspeicher: ≥ 60 GB
- Direkter Internetzugang ohne Proxy zur Freischaltung von KeyCredits und Lizenzen für den Zugriff auf die durch EVVA besicherte authentische und nicht manipulierte Softwareauslieferung
- Lokales LAN mit Low Latency (Ping<10 ms, Roundtrip <30 ms);
  WLAN für die Xesar Tablet-Synchronisierung und Zugriff auf die bereitgestellten Services
- 1 × USB-Host 2.0
- 1 × Codierstation von EVVA mit Slot für die Admin-Karte und mit Unterstützung für kontaktlose RFID-Karten (Mifare Desfire EV1; ISO 14443)
- Tastatur und Maus
- Bildschirmauflösung: 1920 × 1080 Pixel
- Betriebssystem: Windows 10/11 Pro 64-Bit
- HTML5/CSS3-kompatibler Browser, mit Javascript aktiviert
- **Lokales Netzwerk:**
  WLAN (Wireless): IEEE.802.11 g, n
  Protokolle:
  - IPv4
  - HTTP/HTTPS (mit TLS)

Durch EVVA bereitgestellte Services im Internet:

Service	URL: Port	Port Adressen
Trusted Registry	https://sfw.evva.com:443 https://sfw.evva.com:4443	Fix
Lizenzservice	https://license.evva.com:8072	Fix

Service Katalog: Kommunikation Online-Wandleser – Server (Backend):

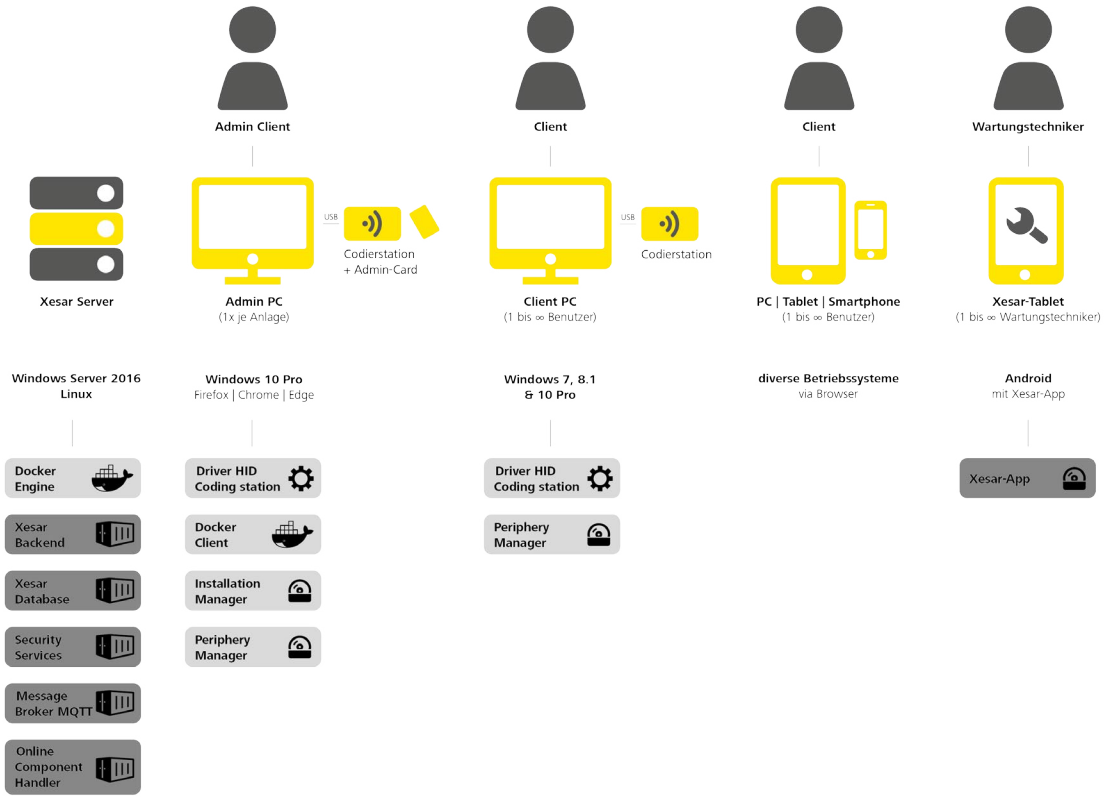
Service	Netzwerk	Default Port	Port Adresse	Protokoll	TLS	Nutzung	Nutzende Kompo-nenten	Bereitstell-ende Kom-ponente
Online Component-Handler	LAN/WLAN	9081	konfigurier-bar	NWP	Ja	Kommunikation mit der Xesar-Software	Xesar-Online-Wandleser	Online-Component-Handler

Folgende Lösungen können möglicherweise realisiert werden (bitte um Rücksprache mit dem EVVA Technischen Büro):

- Betrieb des Installation Managers auf einer virtuellen Maschine
- Betrieb des Installation Managers auf anderen Windows Betriebssystemen
- Einsatz anderer HTML5/CSS3 kompatibler Browser

5.2 Xesar 3.1 Mehrplatz-Anlage

Die Mehrplatz-Anlage besteht aus einem **Server**, einem **Admin-PC mit Codierstation und Admin-Karte** sowie gegebenenfalls weiteren **Client-PCs mit/ohne Codierstation**. Optional können auch **mobile Geräte** über Browserzugang als Client ohne Codierstation verwendet werden. Das **Xesar-Tablet** wird als Wartungsgerät für die Anlagenverwaltung verwendet. Dazu eine Übersicht der verschiedenen Varianten:



5.2.1 Systemanforderungen für Mehrplatz-Anlagen

Für eine Mehrplatz-Anlage ist der Betrieb eines Servers im 24/7-Betrieb Voraussetzung. Folgende Mindestanforderungen müssen erfüllt sein:

- x86-64 kompatibler Prozessor (CPU); mindestens Quad-Core ≥ 1,5-2,3 GHz
- Hardware-Unterstützung für Virtualisierung
- Arbeitsspeicher (RAM): ≥ 16 GB (mit OS; min. 4 GB für den Server Software Stack)
- Festplattenspeicher, SSD empfohlen: ≥ 60 GB (Systemgröße und geplante Laufzeit bei der Dimensionierung beachten)
- Direkter Internetzugang ohne Proxy zur Freischaltung von KeyCredits und Lizenzen für den Zugriff auf die durch EVVA besicherte authentische und nicht manipulierte Softwareauslieferung
- Lokales LAN mit Low Latency (Ping <10 ms, Roundtrip <30 ms)
- WLAN zur Xesar-Tablet-Synchronisation mit dem Server
- Zugriffsmöglichkeit aus dem lokalen LAN auf den Server für bereitgestellte Services
- Docker Engine 1.12.0+ mit Unterstützung für API 1.24 (werden im Zuge der Docker-Installation installiert)

5.2.2 Service Katalog: Management einer Xesar 3 Mehrplatz-Anlage

Siehe Abschnitt „Server-Kommunikation"

- Server – Admin-PC
- Server – Client-PC
- Server – Online-Wandleser

Getestete Betriebssysteme:

OS	OS Typ	Version	Virtualisierung möglich
Ubuntu	Linux	18.04 / 20.04 LTS Server	Ja

Getestete Hypervisor:

OS	Version	Virtualisierung möglich
Windows Server	2016 / 2019 Standard / Datacenter	Nein
VMWare[1]	VMWare ESXi 6.x	Nein

1 Container optimiertes Betriebssystem von VMware empfohlen für VMware vSphere ESXi 6.x

Xesar muss im Betrieb bei der Kommunikation mit den Online-Komponenten Echtzeitanforderungen erfüllen. Im Falle, dass der Windows Server 2016/2019 nicht allein für die Xesar-Software zur Verfügung steht, muss im Betrieb als Hypervisor dafür Sorge getragen werden, dass die notwendigen Ressourcen dauerhaft zugewiesen sind.

Auf Grund der Vielzahl an möglichen Betriebssystemen können nicht alle auf Kompatibilität von EVVA getestet werden.

Falls ein nicht von EVVA getestetes Betriebssystem verwendet werden soll, halten Sie bitte vorher Rücksprache mit dem zuständigen EVVA Technischen Büro.

Auf Grund der fortlaufenden Entwicklungen am IT-Markt erfragen Sie bitte die aktuelle Kompatibilitätsliste bei Ihrem EVVA Partner oder dem Technischen Büro von EVVA.

5.2.3 Systemanforderungen für Administrator-PC mit Codierstation und Admin-Karte

Für den Betrieb der Xesar-Software (Installation-Manager) müssen folgende Mindestanforderungen erfüllt sein:

- x86-64 kompatibler Prozessor (CPU) 1-2-Core 2,4 GHz oder höher
- Unterstützung für Virtualisierung
- Arbeitsspeicher (RAM): ≥ 8 GB (mit OS; min. 1 GB für die Applikationen Installation Manager und Periphery-Manager)
- Festplattenspeicher: ≥ 10 GB
- Direkter Internetzugang ohne Proxy zur Freischaltung von KeyCredits und Lizenzen für den Zugriff auf die durch EVVA besicherte authentische und nicht manipulierte Softwareauslieferung
- Lokales LAN für den Zugriff auf die vom Xesar 3.1-Server bereitgestellten Services
- 1 × USB Host 2.0
- 1 × Codierstation von EVVA mit Unterstützung für Kontaktlose RFID-Karten (Mifare Desfire EV1; ISO 14443) und mit Slot für Admin-Karte
- Tastatur und Maus
- Betriebssystem: Windows 10/11 Pro 64-Bit
- HTML5/CSS3-kompatibler Browser, mit Javascript aktiviert
- Docker Client mit Unterstützung für API 1.24 , Docker Compose 1.10.0+ (werden im Zuge der Docker-Installation am Admin-PC installiert)

5.2.4 Service Katalog: Management einer Xesar 3-Anlage – Administrator-PC – Server

Siehe Abschnitt „Server-Kommunikation".

PC-Betriebssysteme:

OS	Version	Browser	EVVA-verifiziert	EVVA Codier-station
Windows	10 Pro (V 1511 (build 10586))	Firefox, ab Version 97.0.1 Chrome, ab Version 98.0.4758.102 Edge, ab Version 98.0.1106	Ja	Ja

Folgende Lösungen können möglicherweise realisiert werden (bitte um Rücksprache mit dem EVVA Technischen Büro):

- Betrieb des Installation-Managers auf einer virtuellen Maschine am Server (Admin-Karte wird über Client-PC verbunden)
- Betrieb des Periphery-Managers auf anderen Betriebssystemen (nur auf Anfrage)
- Einsatz anderer HTML5/CSS3-kompatibler Browser

5.2.5 Systemanforderungen für Client-PC mit Codierstation ohne Admin-Karte

Für den Betrieb eines Client-PC **mit Codierstation** in der Mehrplatz-Anlage müssen folgende Mindestanforderungen erfüllt sein:

- x86-64 kompatibler Prozessor (CPU) 1-2-Core 2,4 GHz oder höher
- Arbeitsspeicher (RAM): ≥ 4 GB (mit OS; min. 512 MB für die Peripherie-Manager Applikation, 1–2 GB für einen unterstützten Browser)
- Festplattenspeicher: ≥ 2 GB
- lokales LAN mit Zugriff auf die vom Xesar 3.1-Server bereitgestellten Services
- 1 × USB Host 2.0
- 1 × Codierstation von EVVA mit Unterstützung für Kontaktlose RFID Karten (Mifare Desfire EV1; ISO 14443)
- Keyboard und Maus
- Bildschirmauflösung 1920 × 1080 Pixel
- HTML5/CSS3-kompatibler Browser, mit Javascript aktiviert

5.2.6 Service Katalog: Server und Arbeitsplätze im Mehrplatzsystem – Client-PC – Server

Siehe Anhang zur Projekt-Checkliste „Kommunikation Client-PC - Server (Backend)

Betriebssysteme:

OS	Version	Browser	EVVA-verifiziert
Windows	7 Pro, 64-Bit	• Firefox, ab Version 97.0.1 • Chrome, ab Version 98.0.4758.102 • Edge, ab Version 98.0.1106	Ja Ja Ja
Windows	8.1 Pro, 64-Bit		
Windows	10 Pro, 64-Bit		

Folgende Lösungen können möglicherweise realisiert werden (bitte um Rücksprache mit EVVA Technischen Büros):

- Betrieb des Periphery-Managers auf anderen Betriebssystemen (nur auf Anfrage)
- Einsatz anderer HTML5/CSS3-kompatibler Browser

5.2.7 Systemanforderungen für Client-PC ohne Codierstation (PC/Tablet/Smartphone)

Für den Betrieb eines Client **ohne** Codierstation im Mehrplatz-System müssen folgende Mindestanforderungen erfüllt sein:

- x86-64 kompatibler Prozessor (CPU) 1-2-Core 2,4 GHz oder höher
- Arbeitsspeicher (RAM): ≥ 4 GB (mit OS; 1–2 GB für einen unterstützten Browser)
- Festplattenspeicher: ≥ 2 GB
- Lokales LAN für den Zugriff auf die vom Xesar 3.1 Server bereitgestellten Web-Services
- Keyboard und Maus
- Bildschirmauflösung 1920 × 1080 Pixel
- HTML5/CSS3-kompatibler Browser, mit Javascript aktiviert

5.2.8 Service Katalog: Server und Arbeitsplätze im Mehrplatzsystem

Siehe Anhang zur Projekt-Checkliste „Kommunikation Client-PC – Server (Backend)".

Betriebssysteme:

OS	Version	Browser	EVVA-getestet
Windows	7 Pro	• Firefox, ab Version 97.0.1 • Chrome, ab Version 98.0.4758.102 • Edge, ab Version 98.0.1106	Ja
Windows	8.1 Pro		Ja
Windows	10 Pro		Ja

Folgende Lösungen können möglicherweise realisiert werden (bitte um Rücksprache mit EVVA Technischen Büros):

- Vergleichbare Browser auf anderen Betriebssystemen (nur auf Anfrage)
- Einsatz anderer HTML5/CSS3-kompatibler Browser

5.2.9 Systemanforderungen für Netzwerk (Lokales Netzwerk und Internet)

Lokales Netzwerk:
- Fast Ethernet 100Base-TX 100 Mbit, Standard MTU (1500 Bytes) oder besser
- Low-Latency zwischen den verbundenen Bausteinen (Ping < 10 ms, Roundtrip < 30 ms)
- WLAN (Wireless): IEEE.802.11 g, n

Protokolle:
- IPv4
- HTTP/HTTPS (mit TLS)
- MQTT (mit TLS)
- EVVA NWP (mit Transportsicherung; Online-Wandleser)

Durch EVVA bereitgestellte Services im Internet:

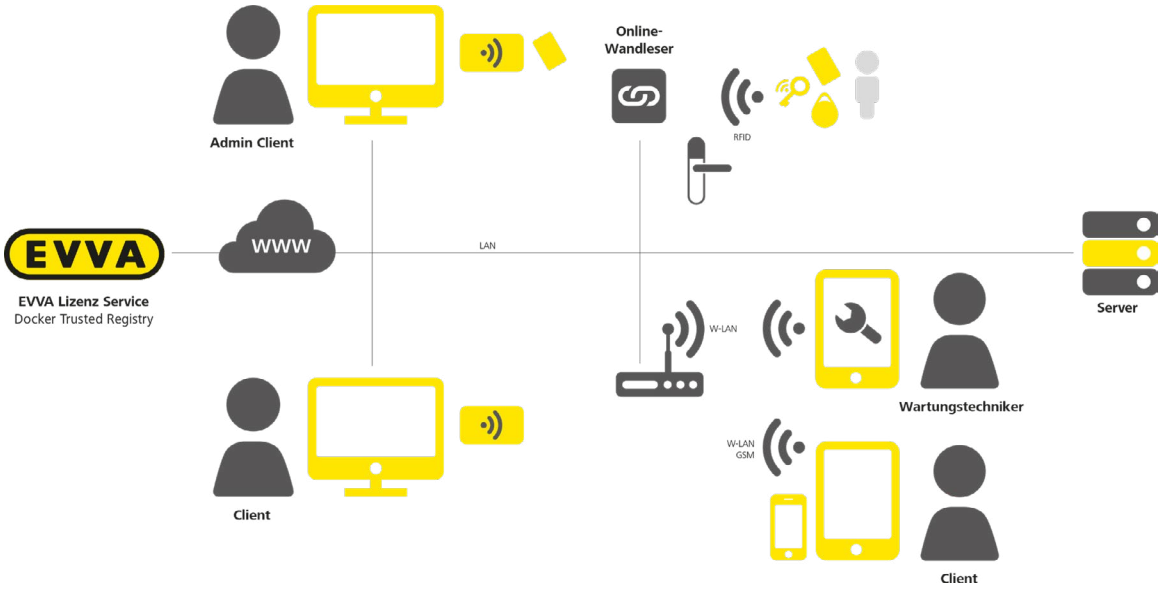
Service	URL	Port konfigurierbar
Trusted Registry	https://sfw.evva.com:443 https://sfw.evva.com:4443	Nein
Lizenzservice	https://license.evva.com:8072	Nein

Durch Xesar 3.1-Server bereitgestellte Services im lokalen Netzwerk:

Service	URL	Was	Port konfi-gurierbar
Docker Engine	tcp://<IP Installation>:2376	Host	Ja
Sicherheitsservice	https://<IP Installation>:8200	Installation	Ja
Message Broker	mqtts://<IP Installation>:1883	Peripherie, Schnittstelle	Ja
Verwaltung	https://<IP Installation>:8080	Betrieb	Ja
Online-Komponenten Handler	tcp://<IP Installation>:9085	Betrieb	Ja

6 Anhang zur Projekt-Checkliste

6.1 Verteilungssicht



6.2 Server-Kommunikation

Anwendung*)	Service	Netzwerk	Default Port	Port Adresse	Protokoll	TLS	Nutzung	Nutzende Komponenten	Bereitstellende Komponente
1;2	Secure Shell (SSH)	LAN/WLAN	22	konfigurierbar	SSH	Ja	Setup und Konfiguration von OS und Docker Engine	Docker-Machine, SSH Client	SSH Service (OS)
1;2	Docker-Engine API Service	LAN/WLAN	2376	konfigurierbar	HTTPS	Ja	Setup der Container und Volumes	Docker-Client	Docker-Engine (Docker, OS)
1;2	Message Broker	LAN/WLAN	1883	konfigurierbar	MQTTS	Ja	Asynchrone Xesar-System Schnittstelle	Installations-Manager	Message Broker
1;2	Service für die Verwaltung von Sicherheitsinformationen	LAN/WLAN	8200	konfigurierbar	HTTPS	Ja	Ablage für Sicherheitsinformationen, Passwörter, Schlüssel	Installations-Manager, Installations-Verwaltung	Vault
3	Docker Trusted Registry sfw.evva.com	WAN	443; 4443	443; 4443	HTTPS	Ja	Bereitstellung von signierten Docker Images und Überprüfung der Signatur	Docker-Client, Docker-Engine	Öffentliche Docker Trusted Registry (Container Image Auslieferung)
4	Lizenzservice license.evva.com	WAN	8072	8072	HTTPS	Ja	Registrieren einer Installation/Admin-Karte und Laden von KeyCredit Codes	Installation-Manager	Lizenzservice
5	Admin-Karte Terminal	USB	Fix	–	ISO 14443	–	Lesen und Schreiben von Zutrittsmedien	Installations-Verwaltung über den Peripherie-Manager (nur Proxy)	Codierstation

Anwendung*)	Service	Netzwerk	Default Port	Port Adresse	Protokoll	TLS	Nutzung	Nutzende Kom-ponenten	Bereitstellende Komponente
6	Installations-Verwaltung Frontend Web Service	LAN/WLAN	8080	konfi-gurier-bar	HTTPS	Ja	Web-Service und Auslie-ferung der Web-Applika-tion für den Browser	Browser	
7	Online Component-Handler	LAN/WLAN	9081	konfi-gurier-bar	NWP	Ja	Kommunika-tion mit der Xesar-Soft-ware	Xesar-Online-Wandleser	Online-Component-Handler

*) **Anwendungen:**

Admin-PC mit Installation-Manager
1: Anlagen Start
2: Anlagen Stopp
3: Anlagen Update
4: Lizenzservice (KeyCredits aufladen)
5: mit Codierstation für Admin-Karte

Client-PC
5: Codierstation für Zutrittsmedien
6: Client-PC Browser-Kommunikation

Online-Wandleser
7: Online-Wandleser Kommunikation

6.3 Kommunikation Client-PC – Server (Backend)

Service	Netzwerk	Default Port	Port Adresse	Protokoll	TLS	Nutzung	Nutzende Kompo-nenten
Installations-Ver-waltung Frontend Web Service	LAN/WLAN	8080	konfigu-rierbar	HTTPS	Ja	Web-Service und Auslieferung der Web-Applikation für den Browser	Browser
Message Broker*	LAN/WLAN	1883	konfigu-rierbar	MQTTS	Ja	Asynchrone Xesar System Schnitt-stelle	Periphery-Manager
Codierstation*	USB	fix	–	ISO 14443	–	Lesen und Schrei-ben von Zutritts-medien	Installations-Verwaltung über den Periphery-Manager (nur Proxy)

* Nur bei Client-PC mit Codierstation

6.4 Kommunikation Online-Wandleser – Server (Backend)

Service	Netzwerk	Default Port	Port Adresse	Protokoll	TLS	Nutzung	Nutzende Kompo-nenten	Bereitstell-ende Kom-ponente
Online Component-Handler	LAN/WLAN	9081	konfigu-rierbar	NWP	Ja	Kommunikation mit der Xesar-Software	Xesar-Online-Wandleser	Online-Component-Handler

7 Upgrade und Updates

Ein Upgrade auf Xesar 3.1 ist nur von Anlagen mit Xesar 2.2 und Xesar 3.0 möglich.

Dies gilt für Firmware und Software.

Für Upgrades auf Xesar 3.1 gelten folgende Voraussetzungen:

Xesar-Software
Betriebssystem des PCs: Windows 10 Pro

Xesar-Tablet
WLAN wird vorausgesetzt

Xesar-Zutrittskomponenten
Nach der Installation müssen die Zutrittskomponenten mit der neuen Firmware aktualisiert werden

Xesar-Wandleser
Prozedere bei Konstellation „Steuereinheit und zwei Xesar-Wandleser":

- Xesar-Wandleser aus der Anlage ausbauen und in den Baustellenmodus versetzen.
- Nach der Installation von Xesar 3.1 die Xesar-Wandleser in die Anlage einbringen.

Admin-Karte
Als Admin-Karte muss die X2.2-Karte verwendet werden

	**Zutrittsmedien** Medien aus Xesar 2.2 Anlagen müssen nach dem Upgrade am Online-Wandleser oder an der Codierstation aktualisiert werden.
	**KeyCredits** Lifetime und Guthaben der Stück KeyCredits werden übernommen. KeyCredits Unlimited 12/36 Monate gehen verloren.

Folgende Tablets werden mit Xesar 3.1 unterstützt:

Xesar-Tablet V2 (Acer Iconia One 7 (B1-770 und B-730HD)
Eingeschänkte Funktionen: keine BLE Funktion, nur Kabelverbindung möglich

Xesar Tablet Ares BLE 4.2
Volle Funktion, BLE und Kabelverbindung

8 Upgrade Xesar 2.2 auf Xesar 3.1

Die Bedienung der Xesar-Software 3.1 unterscheidet sich deutlich von der Bedienung der Xesar-Software 2.2.
Wir empfehlen daher dringend, vor dem Umstieg von Xesar 2.2 auf Xesar 3.1 eine ausführliche Schulung in unserer EVVA-Akademie zu besuchen.
Schulungstermine erhalten Sie beim EVVA-Support.!

Für das Upgrade von Xesar 2.2-Anlagen auf Xesar 3.1 beachten Sie folgende Punkte:

8.1 Vor dem Upgrade

- Eine Xesar 2.2-Anlage kann nur in der gleichen Zeitzone importiert und betrieben werden.
- Die vorhandene Admin-Karte Ihrer Xesar 2.2-Anlage wird weiterverwendet.
- Die bereits vorhandenen Zutrittsmedien können weiterverwendet werden. Sie müssen dazu auf der Codierstation oder einem Online-Wandleser aktualisiert werden.
- Stück KeyCredits können weiterverwendet werden.
- KeyCredit Unlimited (12 bzw. 36 Monate) können bei Xesar 3.1 nicht weiterverwendet werden, sie verfallen!
- Verwenden Sie KeyCredit Xesar Lifetime für die unbeschränkte Verwaltung mit nur einmaliger Bezahlung!
- Die Xesar Lifetime Lizenz darf erst nach erfolgtem Upgrade auf Xesar 3.1 eingelöst werden.
- Führen Sie alle offenen Wartungsaufgaben Ihrer Xesar 2.2-Anlage aus.
- Erstellen Sie zur Sicherheit ein manuelles Backup Ihrer Xesar 2.2-Anlage.
- Erstellen Sie von den Xesar 2.2 Ereignisprotokollen Screenshots.
  Ereignisprotokolldaten können nicht von Xesar 2.2 in Xesar 3.1 übernommen bzw. importiert werden.
- Für eine Xesar 2.2-Anlage mit der Konstellation „Zwei Xesar-Wandleser mit einer Steuereinheit" müssen diese Wandleser vor dem Upgrade auf Xesar 3.x aus der Xesar 2.2-Anlage ausgebaut und in den Baustellenmodus gebracht werden.
  Nach dem Upgrade auf Xesar 3.1 bauen Sie die beiden Wandleser wieder in die Anlage ein.
- Die von Xesar benötigten Ports sind: 8080, 1883, 8200, 9081. Die Firewall darf die benötigten Ports nicht blockieren. Bei Bedarf können die Ports nachträglich geändert werden.
- Auf Ihrem Xesar-Tablet muss die bestehende Xesar-Wartungsapp deinstalliert werden. Die neue Xesar-Wartungsapp 3.1 muss nach dem erfolgreichen Upgrade manuell auf das Xesar-Tablet installiert werden (siehe Kapitel „Manuelle Deinstallation und Installation der Xesar-Wartungsapp").
- Wird eine Xesar 2.2-Anlage mit einem Feuerwehr-Berechtigungsprofil in Xesar 3.1 importiert, kann es vorkommen, dass ein weiteres Feuerwehr-Berechtigungsprofil

erzeugt wird. In diesem Fall muss ein Feuerwehr-Berechtigungsprofil manuell entfernt werden.

- Nachdem eine Xesar 2.2-Anlage nach Xesar 3.1 importiert wurde, dürfen die Komponenten nicht mehr mit der Xesar 2.2-Anlage synchronisiert und nur mehr mit Xesar 3.1 weitergearbeitet werden.
- Nach dem Upgrade werden für alle Komponenten Wartungsaufgaben zum Firmware-Update erzeugt. Dabei wird die aktuelle Firmware der Komponenten für Xesar 3.1 mit dem Xesar-Tablet und der aktuellen Xesar-Wartungsapp auf die Komponenten übertragen.
- Führen Sie diese Wartungsaufgaben zur Funktionssicherheit der Anlage möglichst zeitnah nach dem Upgrade durch.

8.2 Upgradeanleitung Xesar 2.2 auf Xesar 3.1

» Stoppen Sie die Xesar 2.2 Anlage.
» Installieren Sie den neuen Xesar 3.1 Installation-Manager (siehe Installationsanleitung Xesar 3.1).
» Stecken Sie die Admin-Karte Ihrer Xesar 2.2-Anlage in die Codierstation.
» Wählen Sie im Xesar 3.1 Installation-Manager unter PC-Anlagen „Wiederherstellung/Import".
» Laden Sie die Datenbankdatei Ihrer Xesar 2.2-Anlage und folgen Sie den Anweisungen. Die Xesar 2.2 Datenbankdatei finden Sie unter: C:\ProgramData\Xesar 2.2\<Nummer der Admin-Karte>.

Nach dem erfolgreichen Upgrade finden Sie Ihre Anlage unter PC-Anlagen.

Für Hilfe und weitere Informationen wenden Sie sich an Ihren EVVA-Partner oder das Technische Büro von EVVA.

9 Upgradeanleitung einer Xesar 3.0 PC-Anlage auf Xesar 3.1

Für Xesar 3.0-Anlagen auf Server wenden Sie sich bitte vor dem Update an Ihren EVVA-Support

Ansicht Xesar-Anlagen auf PC:
Hier werden PC-Anlagen, die mit dem neuen Installation-Manager installiert wurden, angezeigt und verwaltet. Es können PC-Anlagen aus der Ansicht Server-Anlagen in die Ansicht PC-Anlagen verschoben werden.

Ansicht Xesar Anlagen auf Server:
Die Anzeige ist gleich der vom Xesar 3.0 Installation-Manager. Hier werden Anlagen angezeigt, die von Xesar 3.0 aktualisiert wurden.

9.1 Updateschritte am PC:

- Erzeugen Sie im vorhandenen Installation-Manager mittels manuellen Backup eine aktuelle Backup-Datei.
- Beenden Sie den alten Installation-Manager.
- Installieren Sie den neuen Installation-Manager.
- Stecken Sie die Admin-Karte Ihrer Xesar 3.0-Anlage in die Codierstation.

Sie finden Ihre Xesar-Anlage unter Server-Anlagen.

- Entfernen Sie die Anlage in der Server-Anlagen Ansicht.
- Gehen Sie zurück zur Startseite des neuen Installation-Managers.
- Klicken Sie in der PC-Anlagen Ansicht auf Wiederherstellung/Import und importieren Sie die letzte Backup-Datei der Xesar 3.0-Anlage.
- Folgen Sie den Installationsanweisungen.

Nach dem erfolgreichen Update finden Sie Ihre Anlage unter PC-Anlagen.
Die weitere Verwaltung ihrer Anlage findet unter der Ansicht PC-Anlagen statt.

9.2 Updateschritte am Tablet

» Deinstallieren Sie auf Ihrem Xesar-Tablet die bestehende Xesar-Wartungsapp.

» Installieren Sie die neue Xesar-Wartungsapp 3.1 nach dem erfolgreichen Update manuell auf das Xesar-Tablet (siehe Kapitel „Manuelle Deinstallation und Installation der Xesar-Wartungsapp“).

Unter Xesar 3.1 wird die lokale Docker-Installation nicht mehr benötigt und kann nach erfolgreichem Update deinstalliert werden.

Für Hilfe und weitere Informatinen wenden Sie sich an Ihren EVVA-Partner oder das Technische Büro von EVVA.

10 Installationsanleitung

10.1 Installation des Treibers für die Codierstation

Für den Betrieb der Codierstation (HID Omnikey 5421) am PC ist die Installation des HID Hardwaretreibers notwendig.

Falls Sie die Version HID Omnikey 5422 der Codierstation haben, ist keine Treiberinstallation notwendig. (In diesem Fall direkt mit Kapitel „Xesar 3.1 Programme“ fortfahren.)

Um den Treiber für die Codierstation zu installieren, bestehen folgende Varianten:

- Automatische Treibersuche über Windows
- Manuelle Treibersuche auf der Homepage des Herstellers

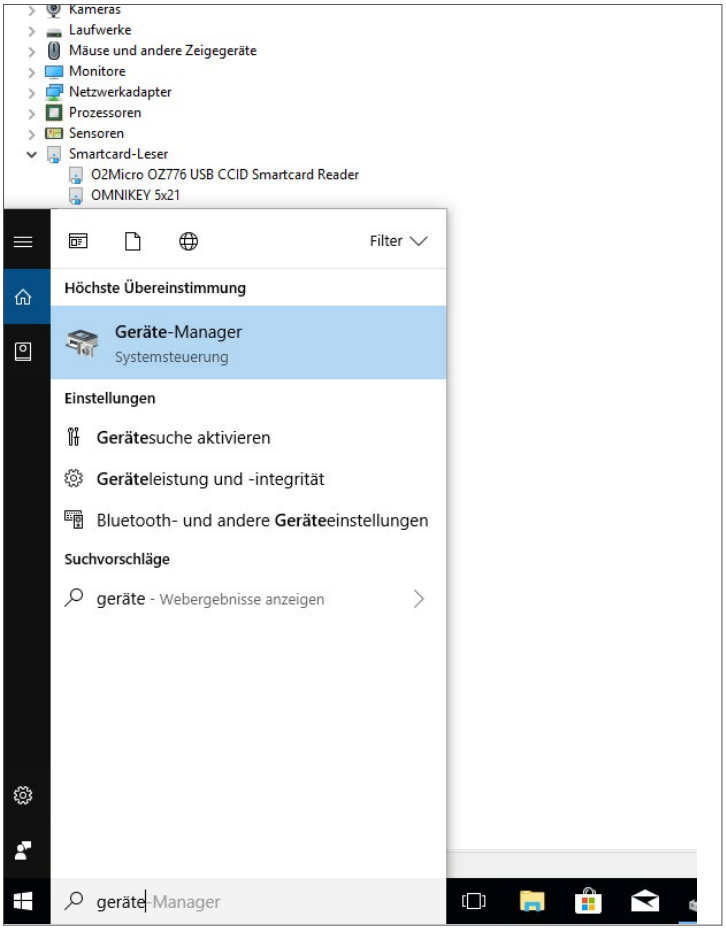
10.1.1 Automatische Treibersuche

Bei Windows 10 wird die Codierstation in der Regel automatisch erkannt. Bei einer PC-Installation wird die angesteckte Codierstation geprüft

Zur Treiberinstallation der Codierstation verwenden Sie den Windows Geräte-Manager.

» **1. Schritt:**
Stecken Sie Ihre Codierstation ohne Admin-Karte an den USB-Anschluss Ihres PC an!

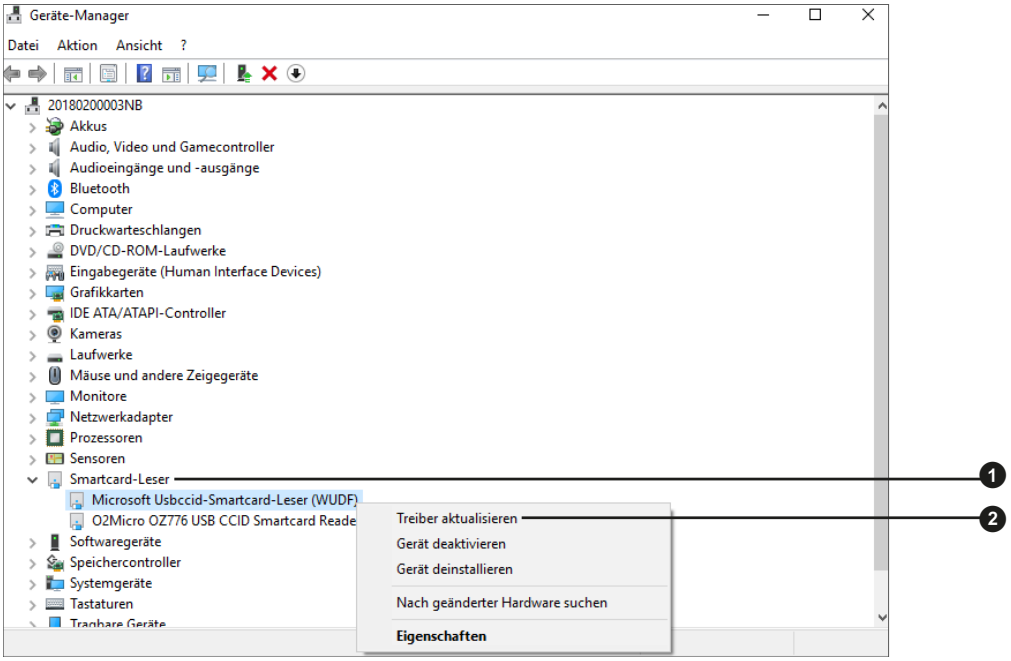
» **2. Schritt:**
Öffnen Sie den „Geräte-Manager" über die Windows Suchleiste.



3. Schritt:

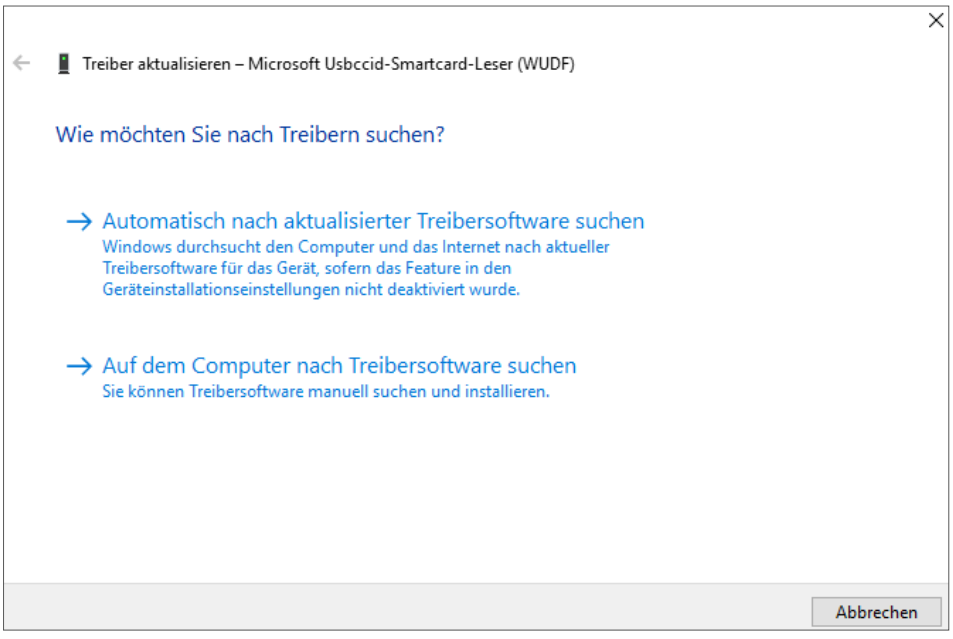
❶ Durchsuchen Sie die Liste nach **Smartcard-Leser** (evtl Reader).
Öffnen Sie diesen Eintrag per Mausklick und wählen Sie den Eintrag aus, der mit **Microsoft ...** beginnt.

❷ Rechtsklick auf den Eintrag **Microsoft...** und **Treiber aktualisieren** wählen.

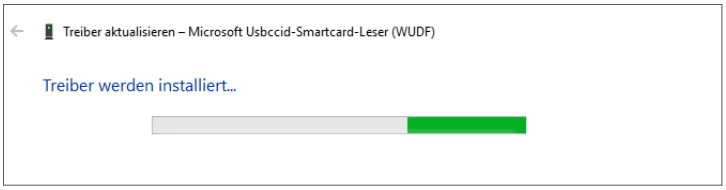


4. Schritt:

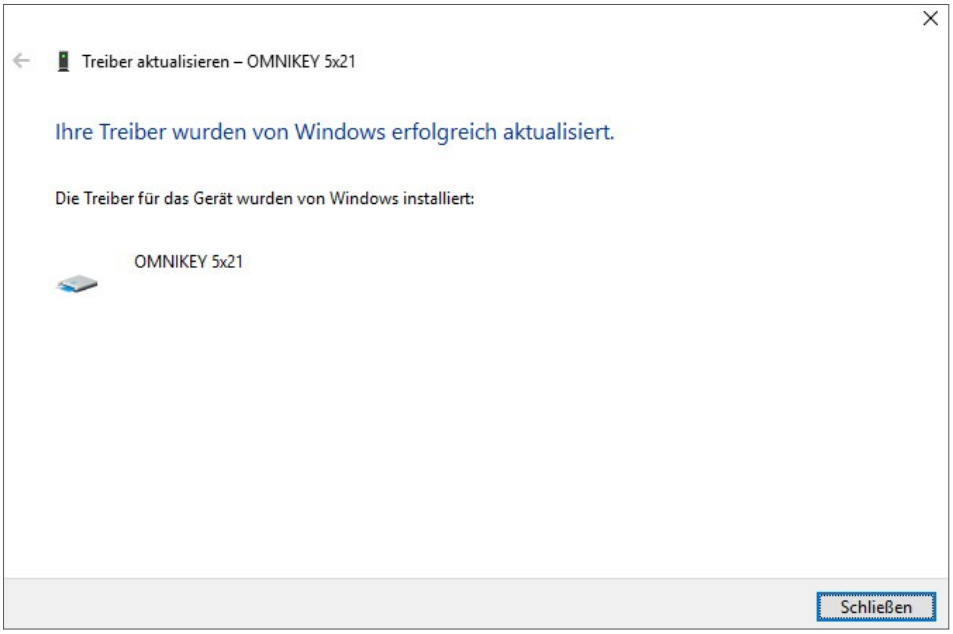
Die Meldung **Automatisch nach aktualisierter Treibersoftware suchen** bestätigen.



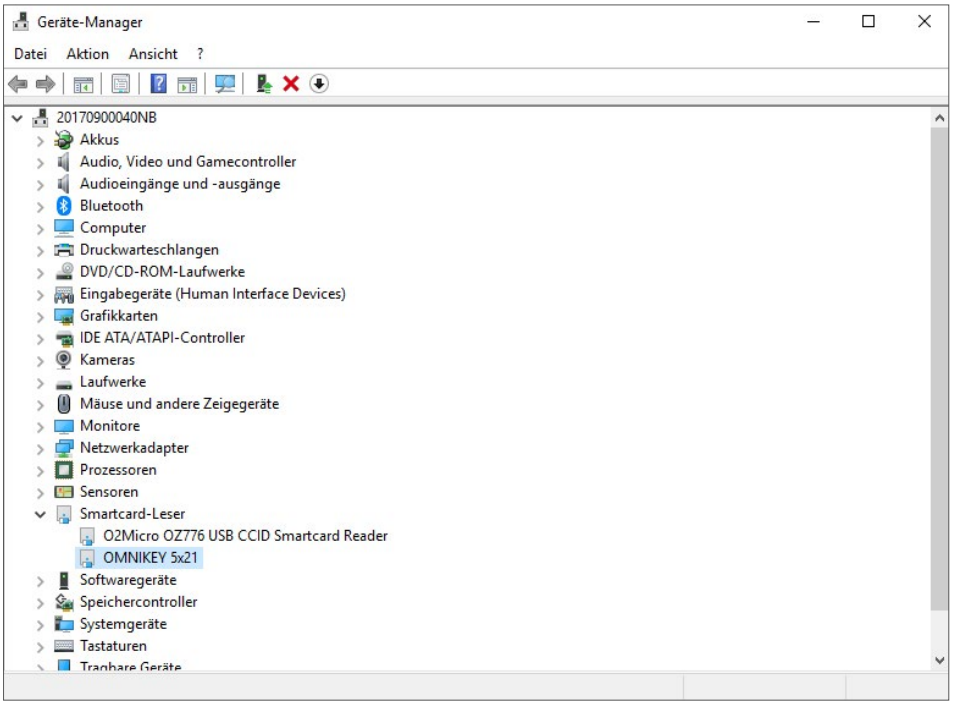
» **5. Schritt:**
Der Treiber wird automatisch heruntergeladen und installiert!



» **6. Schritt:**
Der Treiber wurde installiert. Klicken Sie auf **Schließen**.



Im Gerätemanager ist der verwendete Leser Omnikey 5x21 nun angeführt.



Die Installation des Treibers für die Codierstation ist damit abgeschlossen. Als nächsten Schritt mit Kapitel „Xesar 3.1 Programme fortfahren".

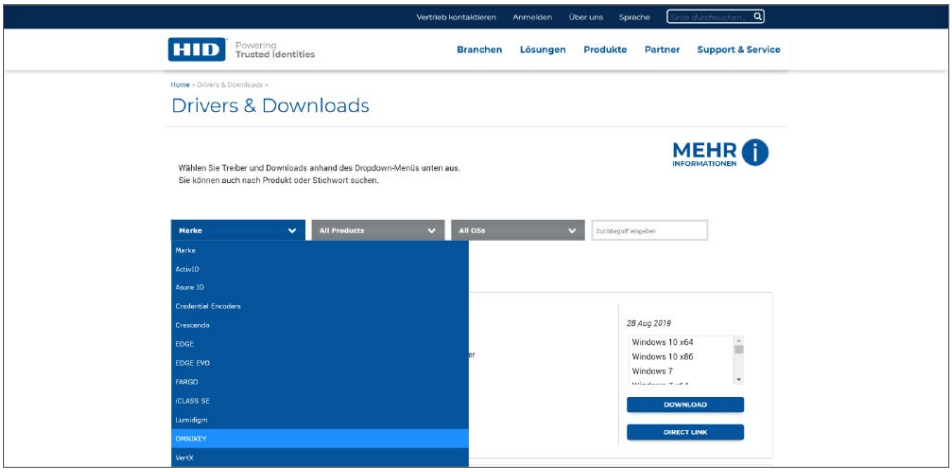
10.1.2 Manuelle Treibersuche

Alternativ zur automatischen Treibersucher besteht die Möglichkeit, den richtigen Treiber direkt auf der Seite von HID Global herunterzuladen.

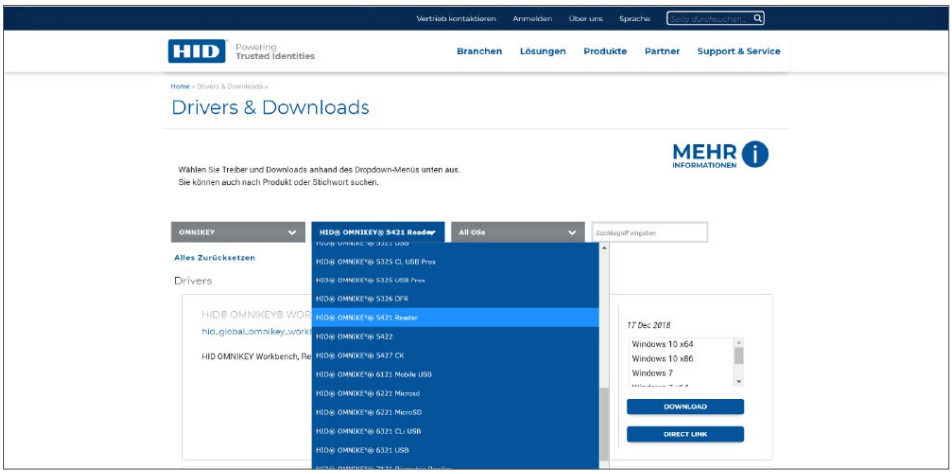
» **1. Schritt:**
Prüfen Sie, den Modelltyp Ihrer Omnikey-Codierstation (auf der Rückseite des Gerätes, z.B. HID OMNIKEY 5421) und stecken Sie die Codierstation an Ihrem PC an.

2. Schritt:
Starten Sie in Ihrem Browser auf der Website von HID Global die Webseite für Treiber:

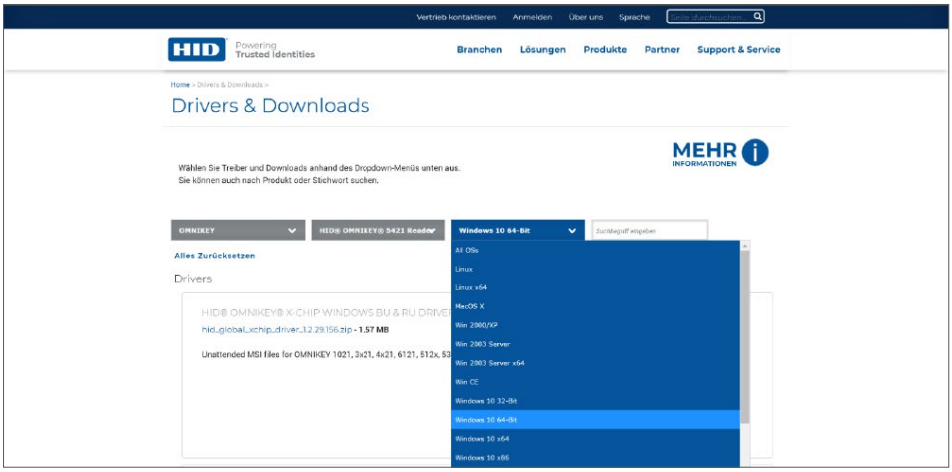
https://www.hidglobal.com/drivers



3. Schritt:
Wählen Sie Ihr Modell (z. B. HID OMNIKEY 5421)

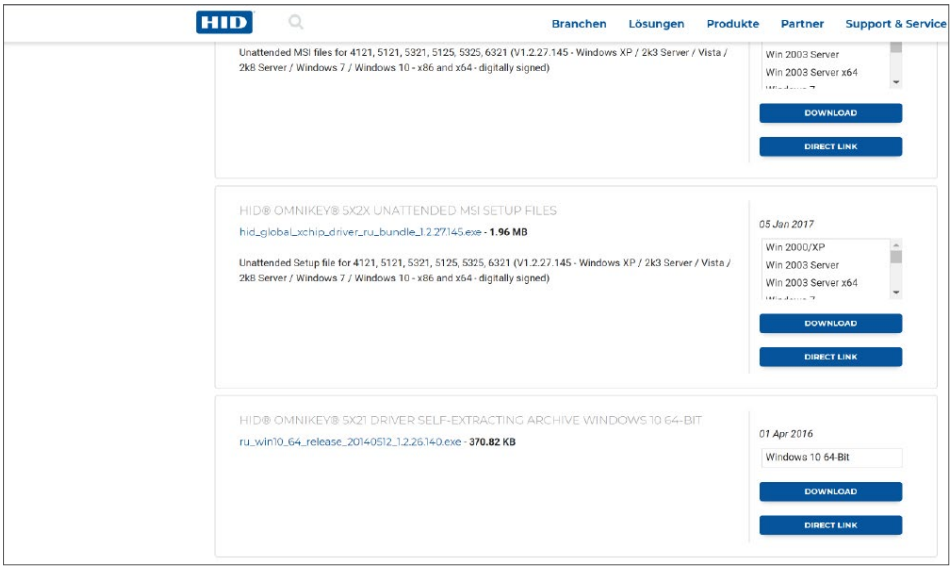


» **4. Schritt:**
Wählen Sie Ihr Betriebssystem **Windows 10-64 Bit** aus.



Unter der Auswahl werden alle möglichen Treiber angezeigt.

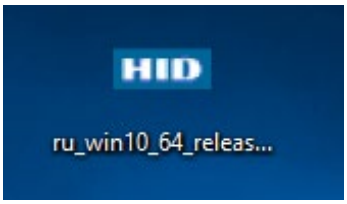
» **5. Schritt:**
Scrollen Sie zum Treiber mit der Bezeichnung „SELF-EXTRACTING ARCHIVE" für Windows 10-64 Bit und klicken Sie auf **Download**.



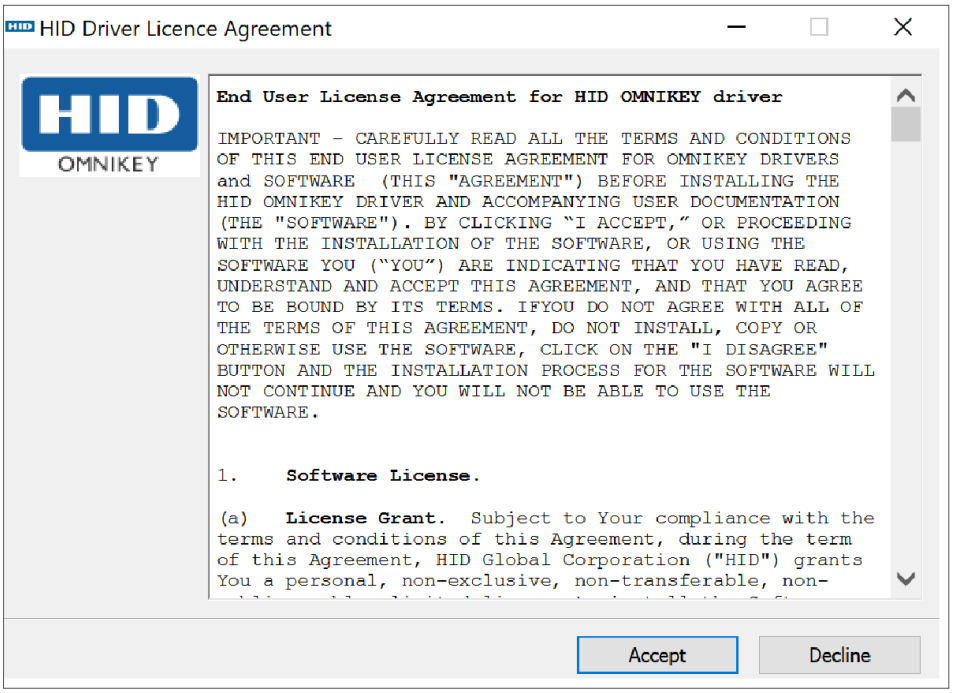
Akzeptieren Sie die Meldung „Download EULA" (End User License Agreement), falls diese eingeblendet wird. Der Download startet.

Sie können die Datei (über „Ausführen") im Browser öffnen und den Installationsprozess starten – in diesem Fall, gehen Sie weiter zum 7. Schritt.

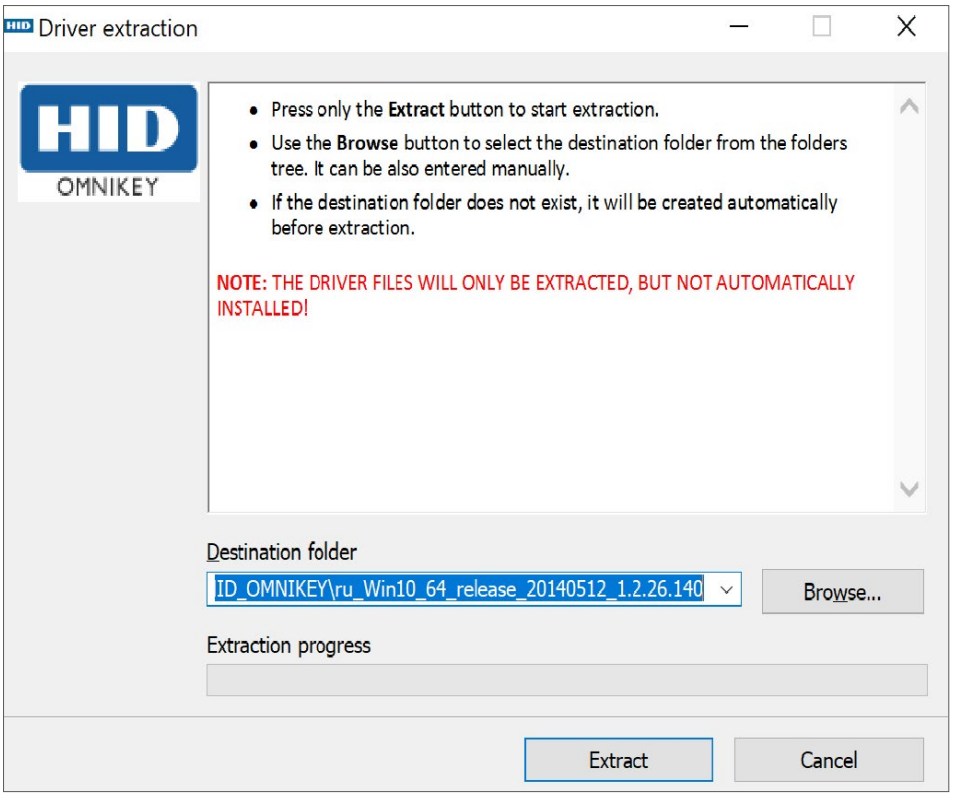
» **6. Schritt:**
Doppelklick auf heruntergeladene Datei



» **7. Schritt:**
Akzeptieren Sie die Meldung „HID Driver Licence Agreement"



» **8. Schritt:**
Es öffnet sich das Fenster „Driver extraction" – klicken Sie auf **Extract**, um den Treiber zu installieren.



Wenn der 8. Schritt abgeschlossen ist, haben sie den HID-Treiber erfolgreich installiert.

11 Installationsanleitung Server mit Ubuntu 20.04

Nachfolgend erhalten Sie Informationen zur Vorbereitung der Xesar 3.1-Installation auf einem Server mit dem Betriebssystem Ubuntu 20.04.

Die Herstellung der notwendigen IT und Serverumgebung ist nicht Teil dieser Installationsanleitung. Diese muss kundenseitig zur Verfügung gestellt werden und liegt nicht in der Verantwortung von EVVA.

» Prüfen Sie die Systemvoraussetzungen für Xesar 3.1. **Vor der Installation müssen Sie bestätigen, dass die Systemvoraussetzungen für Xesar 3.1 laut Projektcheckliste und Systemhandbuch erfüllt sind.**

Beachten Sie die aktuelle Projektcheckliste von EVVA:

› **https://www.evva.com/at-de/xesar/**

Wir empfehlen dringend, die Xesar 3.1-Installation nur in enger Zusammenarbeit mit dem zuständigen IT-Administrator des Betreibers durchzuführen.

11.1 Voraussetzungen

Für eine erfolgreiche Installation von Xesar 3.1 auf einem Server mit dem Betriebssystem Ubuntu 20.04 LTS müssen folgende Voraussetzungen erfüllt sein:

- Admin Client PC WIN 10 PRO mit installierter Docker.Machine.exe und Installation Manager
- Server mit VM Ubuntu 20.04
- Xesar 3.1 Systemanforderungen sind erfüllt

11.2 Ubuntu installieren

Die nachfolgenden Anweisungen gelten für 20.04

» Ubuntu 20.04 downloaden

› **http://releases.ubuntu.com/**

Tutorial zu Ubuntu Installation

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

Bootable USB-Stick

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

» Folgen Sie den Anweisungen bei der Installation

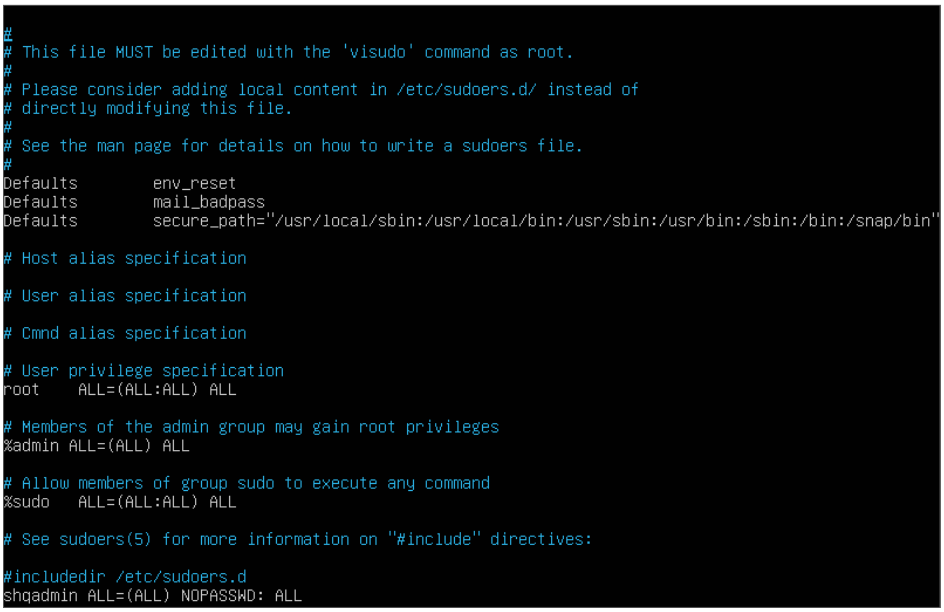
» Nach erfolgreicher Installation von Ubuntu wählen Sie als Option **open ssh server**.

Wenn diese Option nicht zur Auswahl steht, kann sie mit dem Befehl **sudo apt install openssh-server** in der Linux Konsole im Nachhinein installiert werden. Wenn „sudo ohne Passwort" (siehe unten) noch nicht konfiguriert ist, wird das user-Passwort abgefragt.

» Um sudo ohne Passwort einzurichten, geben Sie folgende Befehle in der Linux Konsole ein:

» Befehl **sudo visudo** zur Passwortabfrage für sudo eingeben (Passwort wird abgefragt und das file /sudoers.d wird geöffnet)

» Scrollen Sie bis zum Ende der geöffneten Datei und tippen Sie den Befehl **username ALL=(ALL) NOPASSWD: ALL** unter die letzte Zeile:



- Datei speichern (Strg+O und anschließend ENTER)
- Datei schließen (Strg+X)
- Prüfen Sie, ob das comand **sudo visudo** jetzt ohne Passwortabfrage funktioniert.
- Erstellen Sie in der Linux Konsole ein **SSH Keypair** (Standard ist RSA Verschlüsselung) mit dem Befehl
  ssh-keygen -t ecdsa -b 521 oder **ssh-keygen -t ed25519**.

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

Der SSH Key wird standardmäßig unter /home/user/.ssh auf dem Linuxserver abgelegt. In unserem Beispiel ist der User **shqadmin**, den wir beim Erstellen der Linuxinstallation angelegt haben.

Als nächsten Schritt müssen Sie in der Linux Konsole den erstellten public key (.pub) des keypairs zu den authorisierten Keys auf dem Linux Server hinzufügen.

- Wechseln Sie mit der ersten Kommandozeile ins zuvor erstellte Verzeichnis
- Fügen Sie mit der zweiten Zeile den Key hinzu:
  - **cd /home/user/.ssh**
  - **cat id_ecdsa.pub > authorized_keys**
    cat id_ed25519.pub > authorized_keys

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

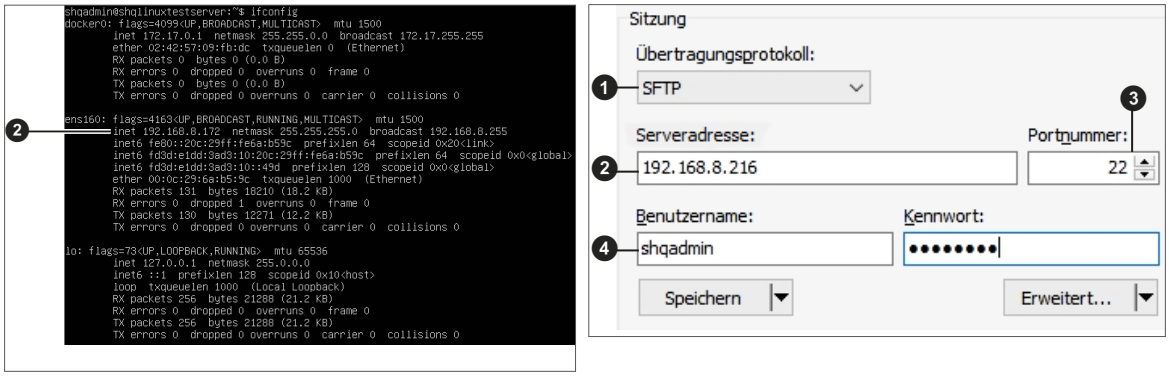
» Installieren Sie ein Programm (z.B. putty oder WINSCP), um Daten sicher vom Client (physischer Win10PRO PC) zum Server und entgegengesetzt zu übertragen). In unserem Beispiel wird WINSCP verwendet.

Freeware-Programm

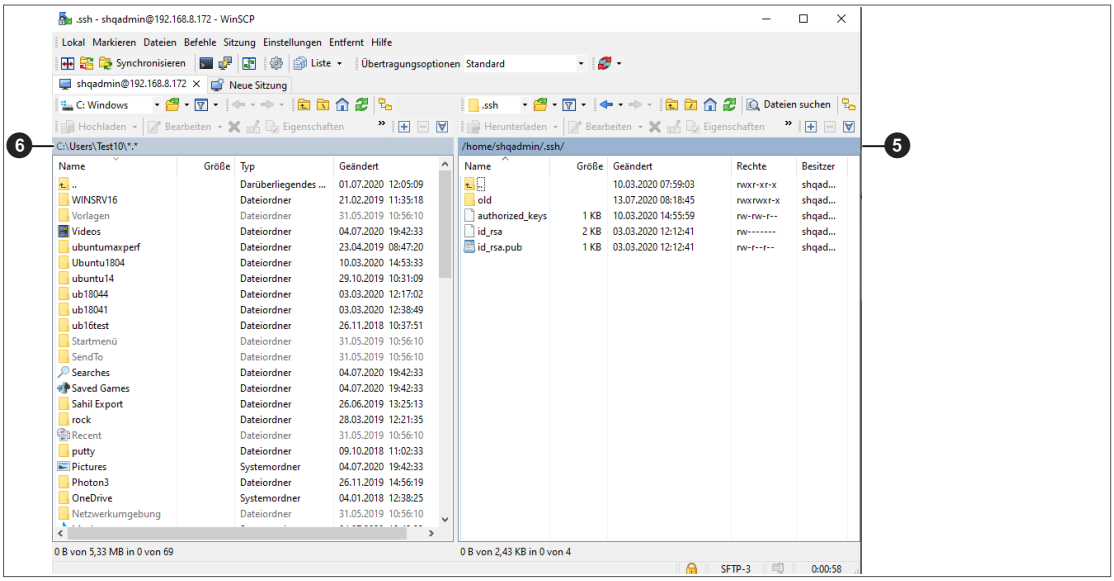
› **https://winscp.net/eng/download.php**

» Mittels WINSCP am Server einloggen

Übertragungsprotokoll ❶ ist SFTP
Rechnername ❷ ist die IP-Adresse des Servers (kann in der Linux Konsole mit dem Befehl **ifconfig** ermittelt werden)
Port ❸ ist 22 (Standard)
Benutzer und Kennwort ❹ entsprechen dem User und seinem Kennwort am Linux Server



» Den Private Key **id_ecdsa / ed25519** und Public Key **id_ecdsa / ed25519.pub** mittels WINSCP auf den Client kopieren.
(In unserem Beispiel von /home/shqadmin/.ssh ❺ am Server nach C:/Users/Test10 ❻ auf den WIN10 Client – Test10 ist der Name des Users auf unserem physischen WIN10 PC.)



» Windows Konsole öffnen
(Mit **cmd** in Suche, Rechtsklick als Admin ausführen)

» Mit dem Befehl **cd C:/Users/Test10** in der Windows Konsole in das Verzeichnis, in dem der Private Key id_rsa abgelegt wurde, wechseln (dieser kann je nach Angabe abweichen)

```
C:\WINDOWS\system32>cd C:/Users/Test10
```

11.3 Docker Maschine erstellen

» Geben Sie den Befehl zur Erstellung der Docker-Maschine in die Windows Konsole ein (ebenfalls aus dem Verzeichnis, in dem der Public Key liegt)

```
C:\Users\Test10>docker-machine create --driver generic --generic-ip-address=192.168.8.216 --generic-ssh-key=id_rsa --generic-ssh-user=shqadmin xs3ubuntu1804
Running pre-create checks...
Creating machine...
(xs3ubuntu1804) Importing SSH key...
Waiting for machine to be running, this may take a few minutes...
Detecting operating system of created instance...
Waiting for SSH to be available...
Detecting the provisioner...
Provisioning with ubuntu(systemd)...
Installing Docker...
Copying certs to the local machine directory...
Copying certs to the remote machine...
Setting Docker configuration on the remote daemon...
Checking connection to Docker...
Docker is up and running!
To see how to connect your Docker Client to the Docker Engine running on this virtual machine, run: docker-machine env xs3ubuntu1804
```

Der Befehl lautet generell:

docker-machine create --driver generic --generic-ip-address (IP Adresse des Servers) --generic-ssh-key (Name des Public keys) --generic-ssh-user (Name des users der für Ubuntu Server erstellt wurde) (Name der docker machine)

Befehlsteil	Erklärung
docker-machine create	ist der generelle Befehl zum Erstellen einer Docker Maschine
--driver generic	ist der generische Treiber zum Installieren von Docker auf dem Server
--generic-ip-address	ist die IP Adresse des Servers
--generic-ssh-key	ist die Angabe des verwendeten Public Keys. (Wenn aus dem Verzeichnis, in dem er abgelegt ist, ausgeführt wird. Bei einem anderen Verzeichnis muss der ganze Pfad angegeben werden.)
--generic-ssh-user	ist Angabe des ssh users (in unserem Beispiel „shqadmin“). Mit einem Abstand folgt der Name der Docker Maschine (in unserem Beispiel xs3ubuntu1804).

Der gesamte Vorgang docker-machine create dauert je nach Rechner ca. 2 bis 10 Minuten.

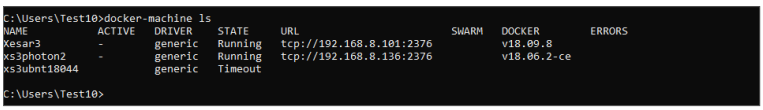
Sollte es zu einer unerwarteten Fehlermeldung kommen, können Sie den Prozess durch Beenden der Windows Konsole abbrechen.
Öffnen Sie anschließend die Windows Konsole erneut und löschen Sie die nicht korrekt erstellte docker machine mit dem Befehl **docker-machine rm „name“** (name ist der vergebene Name).
Beispiel: docker-machine rm xs3ubuntu1804

» Danach geben Sie den Befehl d**ocker-machine --debug create --driver generic --generic-ip-address (IP Adresse des Servers) --generic-ssh-key (Name des Public keys) --generic-ssh-user (Name des users der für Ubuntu Server erstellt wurde) (Name der docker machine)** ein.
Verwenden Sie den Zusatz --debug, um eine genaue Fehlerausgabe zu erhalten.

Bei einer Fehlermeldung in Bezug auf die **ssh Verbindung**, prüfen sie nochmals den user mit **sudo** ohne Passwort bzw. die Ablage der **ssh-keys**.

Bei einer Fehlermeldung in Bezug auf **docker** (z.B. sudo get docker version not found oder ähnlich), versuchen Sie Docker in der Linux Konsole mit dem Befehl **sudo apt install docker.io** manuell zu installieren.

» Nach erfolgreicher Erstellung der Docker-Maschine überprüfen Sie in der Windows Konsole mit dem Befehl **docker-machine ls,** ob die docker-machine auch läuft.

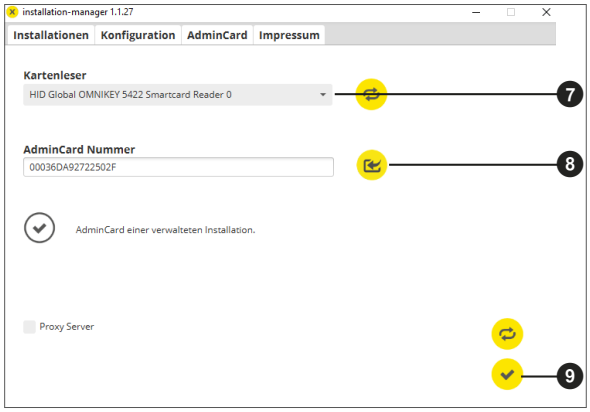


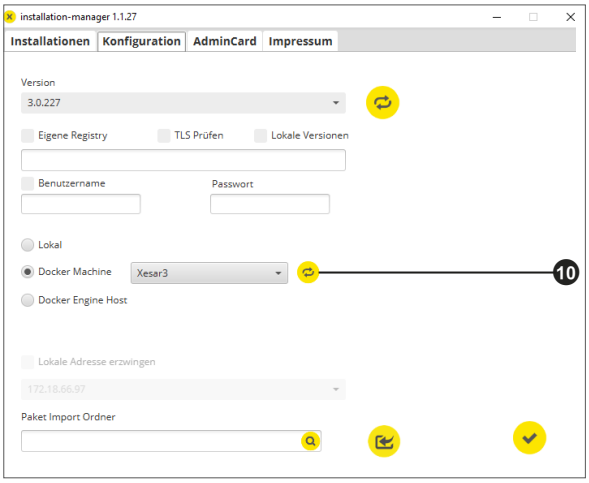
11.4 Xesar 3.1 Installation

- Laden Sie die aktuelle Xesar 3.1-Software herunter

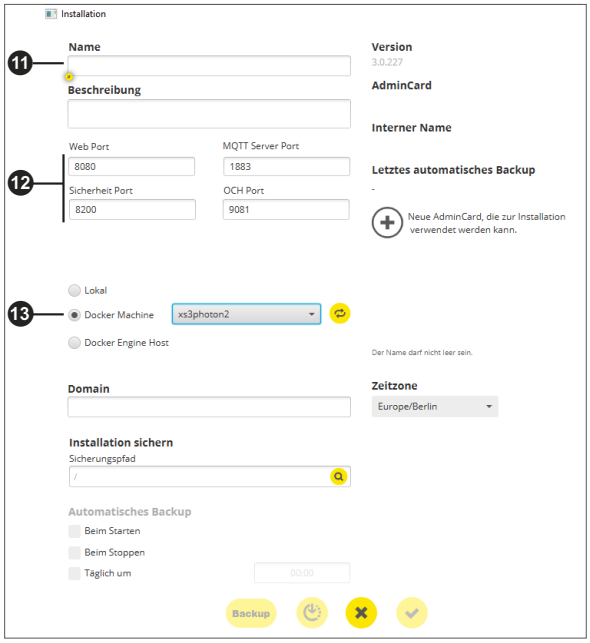
  https://www.evva.com/at-de/produkte/elektronische-schliess-systeme-zutrittskontrolle/xesar/xesar-software-download/

- Codierstation anstecken
- Öffnen Sie den Installation-Manager
- Wählen Sie den Tab **AdminCard**
- Wählen Sie den benötigten Karten-leser ❼
- Laden Sie die Admin-Karte ❽
- Klicken Sie auf den Button ❾, um die Nummer der Admin-Karte einzulesen
- Wählen Sie den Tab **Konfiguration**
- Wählen Sie die Docker Machine ❿





- Wählen Sie den Tab **Installations**
- Fügen Sie mit „+" eine neue Instal-laton hinzu
- Wählen Sie den Namen ⓫, den Port ⓬ sowie die Docker Machine ⓭ aus



Bei einem Update von Xesar 2.2 geben Sie den Datenbankpfad für den Import ein.
Nach Abschluss der Anlagen-Erstellung können Sie die Anlage starten und in Betrieb nehmen (siehe Systemhandbuch).

11.5 Daten-Sicherung

Folgende Daten müssen gesichert werden:

- **Administator-PC** (Windows 10 PRO physischer PC).
  [XesarUser] ist dabei ein Platzhalter für den Windows User (z.B. admin), mit dem die Xesar 3.1-Installation durchgeführt wurde

  - C:System\Users\[XesarUser]\.xesar-1.0.XX\system name
  - C:System\Users\[XesarUser]\.xesar-cs
  - C:System\Users\[XesarUser]\.docker
  - ssh key

Im Installation-Manager können manuelle und automatische Datensicherungen (Backup) durchgeführt werden.

- **VM Server**

  - Snapshot der VM nach jeder größeren oder wichtigen Änderung
  - Generell eine Spiegelung der ganzen Partition, besser der kompletten Festplatte, auf der die Xesar VM (z.B. Ubuntu) installiert ist – im Normalfall bei Servern üblich
  - ssh key

- **Server physisch**

  - komplette Festplatte

12 Installationsanleitung Windows Server 2019 Datacenter Hypervisor

Nachfolgend erhalten Sie Informationen zur Vorbereitung der Xesar 3.1-Installation auf einem Windows-Server mit dem Betriebssystem Versionen Windows Server 2019 Standard oder Datacenter als Hypervisor.

Die Herstellung der notwendigen IT und Serverumgebung ist nicht Teil dieser Installationsanleitung. Diese muss kundenseitig zur Verfügung gestellt werden und liegt nicht in der Verantwortung von EVVA.

» Prüfen Sie die Systemvoraussetzungen für Xesar 3.1. **Vor der Installation müssen Sie bestätigen, dass die Systemvoraussetzungen für Xesar 3.1 laut Projektcheckliste und Systemhandbuch erfüllt sind.**

Beachten Sie die aktuelle Projektcheckliste von EVVA:

› **https://www.evva.com/at-de/xesar/**

Wir empfehlen dringend, die Xesar 3.1-Installation nur in enger Zusammenarbeit mit dem zuständigen IT Administrator des Kunden durchzuführen.

12.1 Voraussetzungen

Ein physischer Server wird mit Microsoft Windows Server 2019 aufgesetzt und als Hypervisor konfiguriert. Auf diesem wird eine VM mit aktuellem Ubunu LTS Server installiert, auf welchem in weiterer Folge Docker mit Xesar 3.1 läuft.

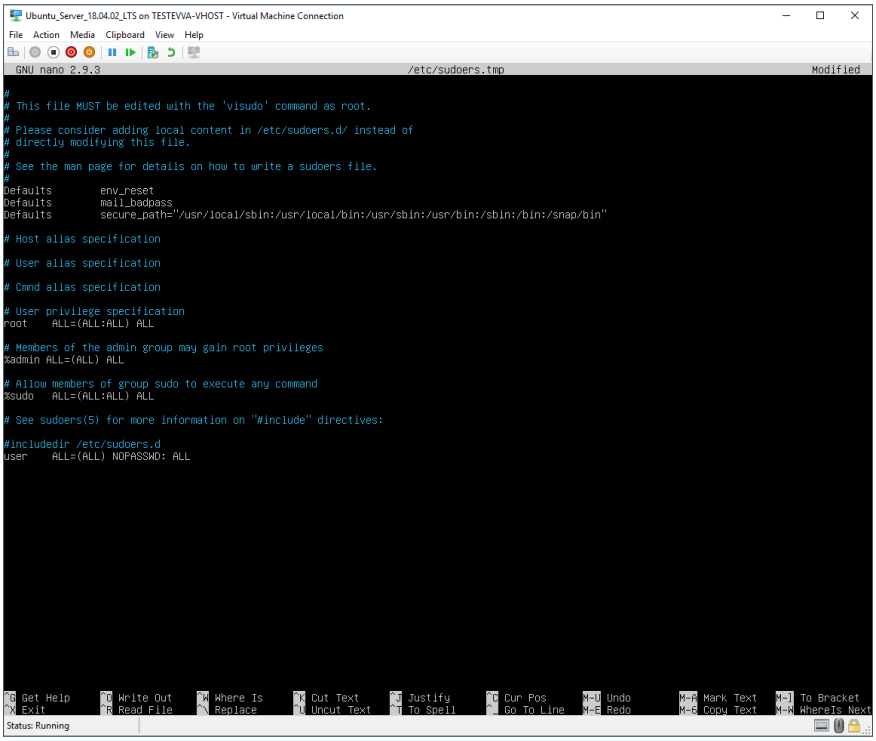
Für eine erfolgreiche Installation von Xesar 3.1 auf einem Server mit dem Betriebssystem Windows Server 2019 müssen folgende Voraussetzungen erfüllt sein:

- Ein physischer Server mit installiertem Windows Server 2019 /Datacenter Betriebssystem ab Version 1607
- Konfiguration als Hypervisor für VM (virtuelle Maschine) für Ubuntu LTS Server für Docker
- Der Anwender (Kunde) verfügt über Windows Server- und Netzwerkverwaltungs-Know-how
- Der Anwender (Kunde) besitzt lokale Administrationsrechte
- Es gibt ein bestehendes DHCP-Service (Dynamic Host Configuration Protocol)
- Die Server-Zeitzone ist als UTC (Coordinated Universal Time) konfiguriert
- Eine Hyper-V-Unterstützung sowie ein virtueller Switch mit Möglichkeit zur Verbindung und Zugriff auf das Internet sind vorhanden
- Internetzugriff (Docker Trusted Registry mit Notary Service und Lizenzservice, Port 443, 4443, 8072) ist vorhanden
- Gegebenenfalls muss der Treiber für die Codierstation installiert werden (HID Omnikey 5422 wird meistens automatisch erkannt)

Aufgrund der Ressourcenverfügbarkeit in Verbindung mit Windows Server empfehlen wir für den physischen Server 16 GB (min. 8 GB). Für die VM werden mindestens 4 GB Speicher benötigt.
Grundsätzlich gilt: je größer die Anlage und mehr Personen bzw.Traffic und Online Wandleser, desto mehr Speicher soll zur Verfügung stehen.

12.2 Ubuntu einrichten

- Befehl **sudo visudo** zur Passwortabfrage für sudo eingeben
- Der nun geöffneten Datei am Ende folgende Zeile hinzufügen:
  user ALL=(ALL) NOPASSWD: ALL
- Den unterstrichenen Bereich durch den Namen des Benutzers ersetzen, der bei der Installation angegeben wurde



- Datei speichern (Strg+O und anschließend ENTER)
- Datei schließen (Strg+X)

- SSH-Schlüsselpaar mit Befehl **ssh-keygen** erstellen
  Name und Passwort können leer gelassen werden – mit ENTER bestätigen

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

- SSH Public Key zu den authorized Keys hinzufügen:
  - **cd /home/user/.ssh/**
  - **cat id_ecdsa.pub > authorized_keys**
    cat id_ed25519.pub > authorized_keys
- Den unterstrichenen Bereich durch den Namen des Benutzers ersetzen, der bei der Installation angegeben wurde

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

12.3 Ubuntu Updates installieren

Mit den folgenden Befehlen werden aktuelle Updates heruntergeladen, installiert und anschließend neu gestartet:

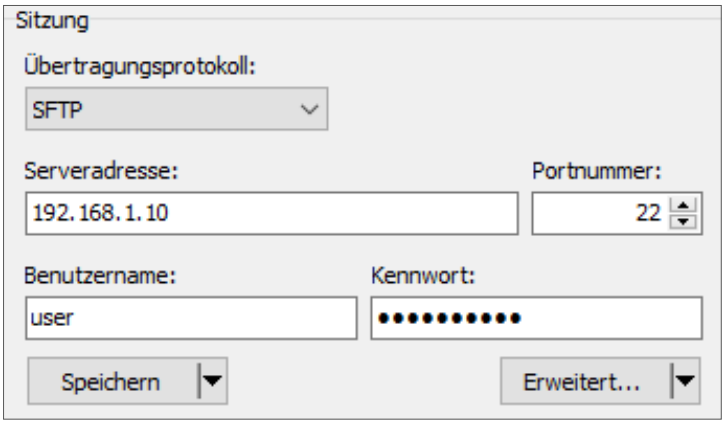
- **sudo apt-get update**
- **sudo apt-get upgrade**
- **sudo apt-get dist-upgrade**
- **sudo apt-get autoremove**
- **sudo reboot now**

12.4 Windows 10 Pro Administrator-PC einrichten

- Herunterladen und installieren WINSCP (Windows Secure Copy), um den SSH Schlüssel zu übertragen.

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

- WINSCP starten
  Dazu benötigen Sie den Rechnernamen, Port, Benutzernamen und das Kennwort des zuvor erstellten Ubuntu Servers.



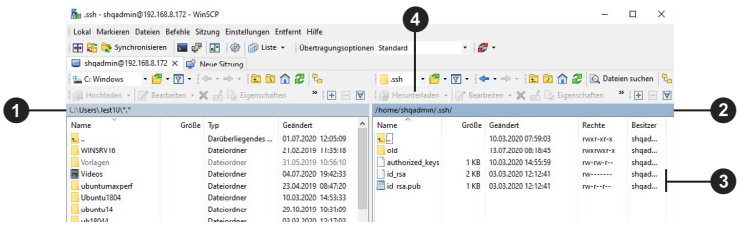
- Die in WINSCP versteckten Dateien und Ordner anzeigen (Strg+Atl+H).

- Zu einem Ordner auf dem lokalen Windows PC (auf der linken Seite ❶) wechseln.

- Auf der rechten Seite ❷ in den Ordner „.ssh" am Ubuntu Server wechseln.

- Dateien „id_rsa" und „id_rsa.pub" ❸ auswählen

- Klicken Sie auf **Herunterladen** ❹, um die ausgewählten Dateien auf den Windows PC zu laden.



- Anschließend die aktuelle Version von Docker CE herunterladen und installieren.

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

- Windows PC neu starten.

» Installation überprüfen.

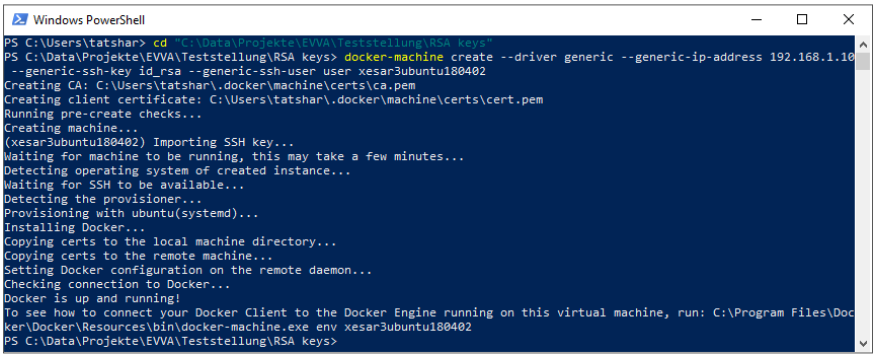
```
PS C:\Users\tatshar> docker version
Client: Docker Engine - Community
 Version:           18.09.2
 API version:       1.39
 Go version:        go1.10.8
 Git commit:        6247962
 Built:             Sun Feb 10 04:12:31 2019
 OS/Arch:           windows/amd64
 Experimental:      false

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

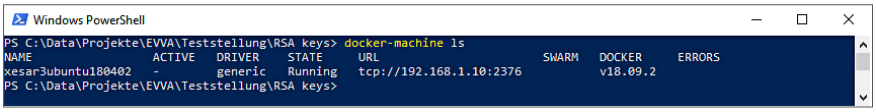
Mit den folgenden Befehlen in der Powershell oder der Windows Konsole wird die Docker Maschine erstellt:

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

- Ersetzen Sie **C:\Data\Projekte\EVVA\Teststellung\RSA keys** durch den Pfad, in den Sie vorher die Dateien mit WINSCP kopiert haben
- **192.168.1.10** ist die IP-Adresse des Ubuntu Servers, die bei der Installation statisch vergeben wurde
- **user** ist der Benutzername des Ubuntu Servers, der bei der Installation angelegt wurde
- **xesar3ubuntu180402** ist der Name, den die Docker Maschine erhalten soll



» Prüfen Sie mit dem Befehl **docker-machine ls**, ob die Docker Maschine läuft



» Schließen Sie die **Codierstation** über USB an ihrem Administrator-PC an

» Stecken Sie die **Admin-Karte** in den Kartenslot der Codierstation.

12.5 Xesar 3.1 Installation

» Laden Sie die aktuelle Xesar 3.1-Software herunter

› **https://www.evva.com/at-de/produkte/elektronische-schliesssysteme-zutrittskontrolle/xesar/xesar-software-download/**

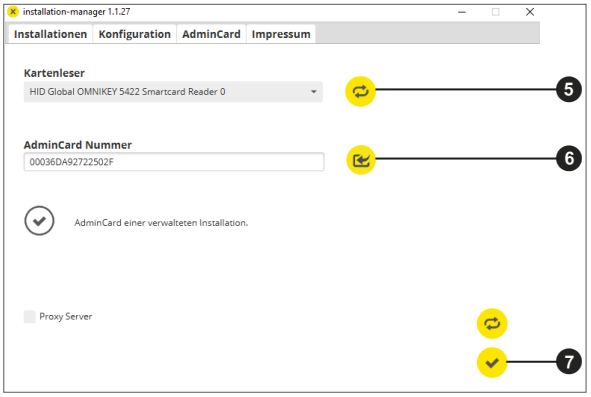
» Öffnen Sie den Installation-Manager

» Wählen Sie den Tab **AdminCard**

» Laden Sie den Kartenleser ❺

» Laden Sie die Admin-Karte ❻

» Bestätigen Sie die Eingabe ❼

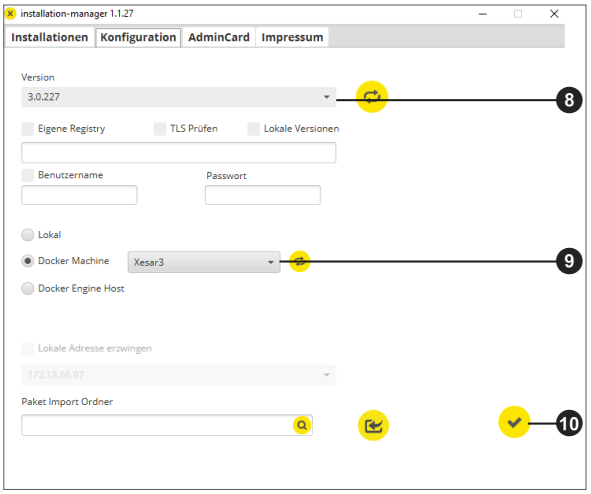


» Wählen Sie den Tab **Konfiguration**

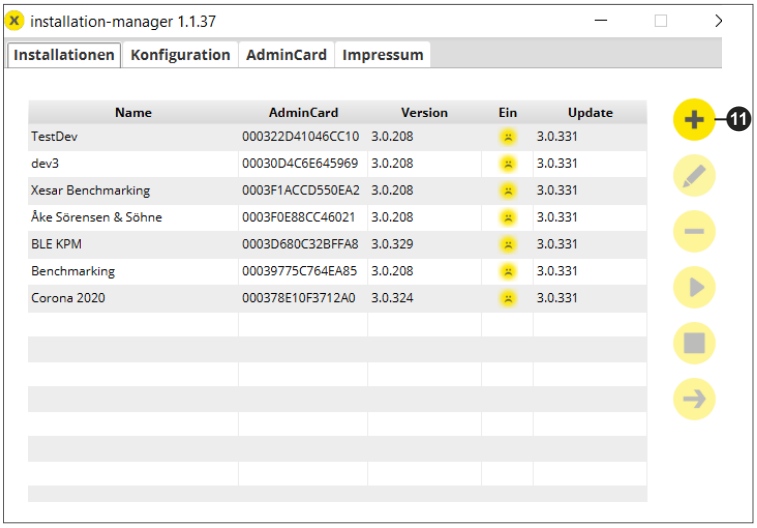
» Wählen Sie die Xesar-Software Version ❽ aus

» Wählen Sie die zuvor erstellte Docker Machine ❾

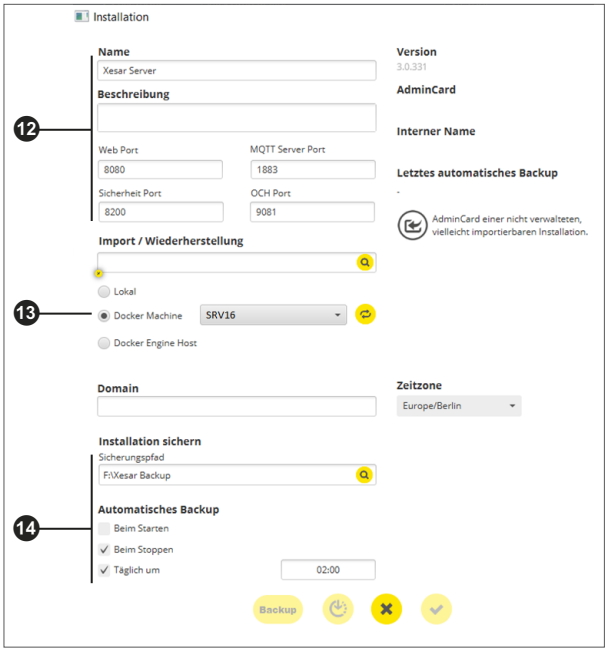
» Bestätigen Sie die Eingabe ❿



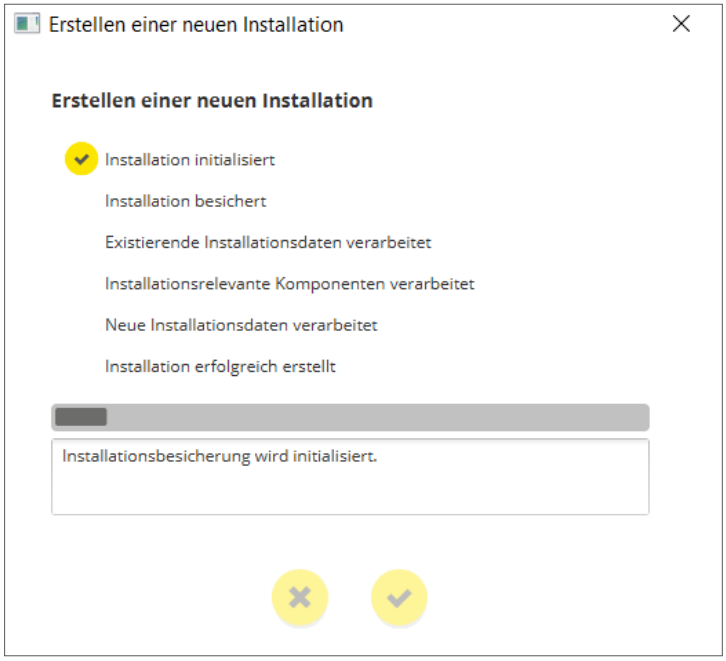
- Wählen Sie den Tab **Installations**
- Fügen Sie mit „+" ⓫ eine neue Anlage hinzu



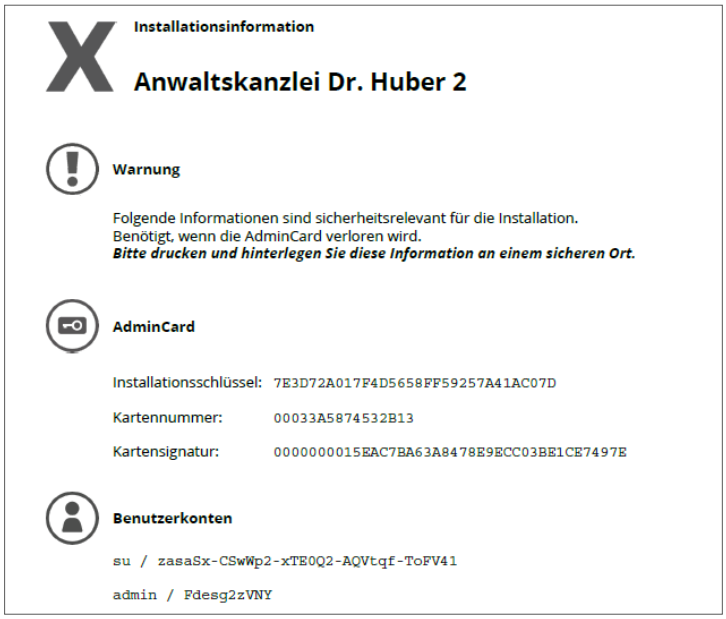
- Füllen Sie alle Daten aus ⓬
- Wählen Sie die Docker Machine ⓭
- Richten Sie die automatische Sicherung ⓮ ein



Die Anlage wird erstellt (es werden wichtige Installationsinformationen angezeigt).

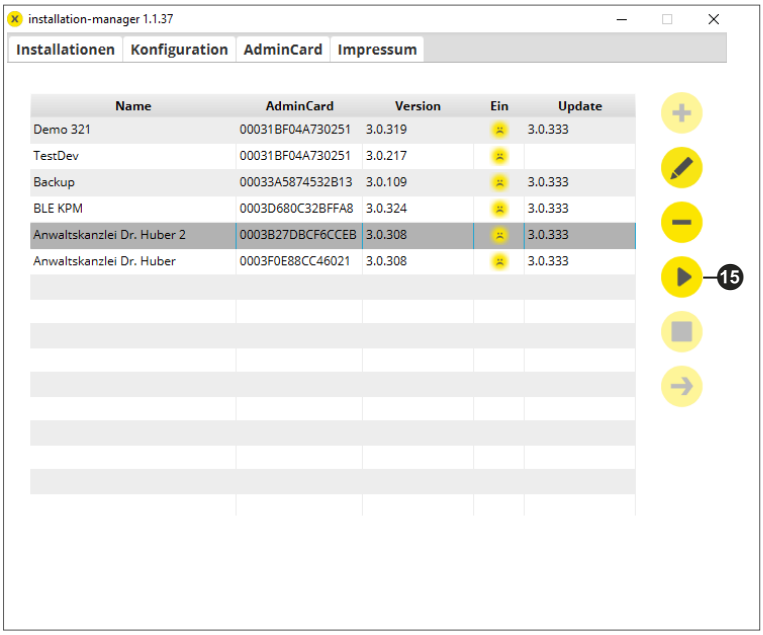


Die wichtigen Anlagendaten werden im Dokument „Installationsinformationen" ausgegeben.

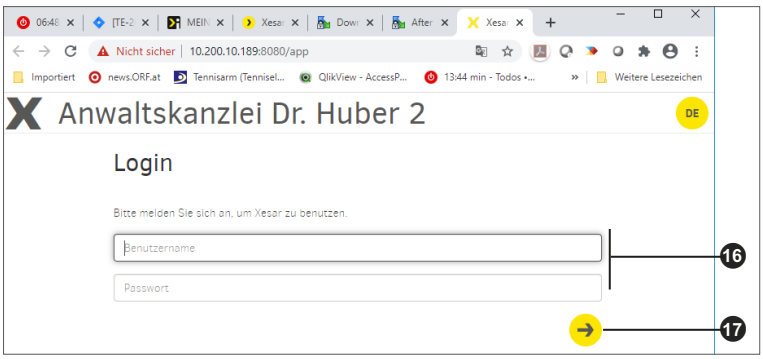


Wichtig:
Ohne diese Daten kann die Anlage im Fehlerfall nicht wiederhergestellt werden. Drucken Sie das Dokument „Installationsinformationen" aus und bewahren Sie es an einem sicheren Ort auf.

- Wählen Sie die gewünschte Anlage aus
- Starten Sie durch Klick auf das Pfeil-Symbol ⓯



- Loggen Sie sich mit den im Dokument „Installationsinformationen" erhaltenen Login-Daten (admin / Passwort) ein ⓰
- Klicken Sie auf das Pfeil-Symbol ⓱



Sie gelangen nun zum Xesar 3.1-Dashboard und können die Anlage bedienen.

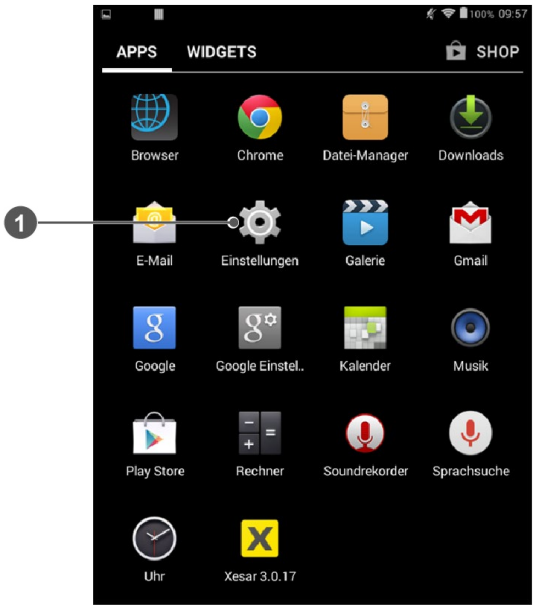
13 Manuelle Deinstallation und Installation der Xesar-Wartungs-app

(Upgrade von Xesar 2.2 oder 3.0 auf Xesar 3.1)

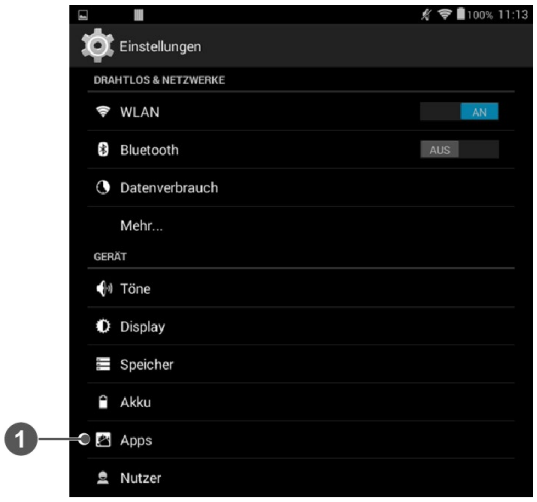
Bei einem Upgrade von Xesar 2.2 oder 3.0 auf Xesar 3.1 muss am Tablet die alte Wartungsapp manuell deinstalliert und die neue Xesar 3.1 Wartungsapp manuell installiert werden.

» Starten Sie Ihr Xesar-Tablet und führen Sie folgende Schritte durch:

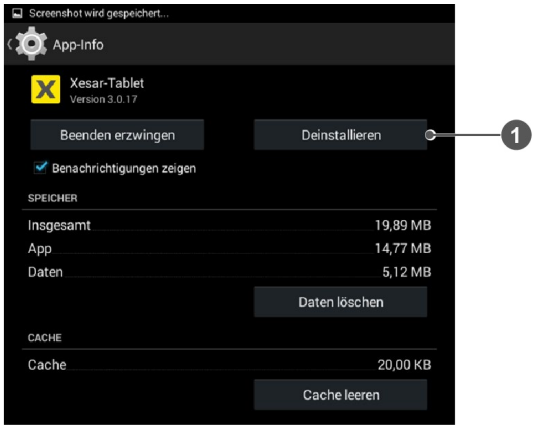
» **1. Schritt:**
Klicken Sie auf Einstellungen ❶ im Hauptmenü



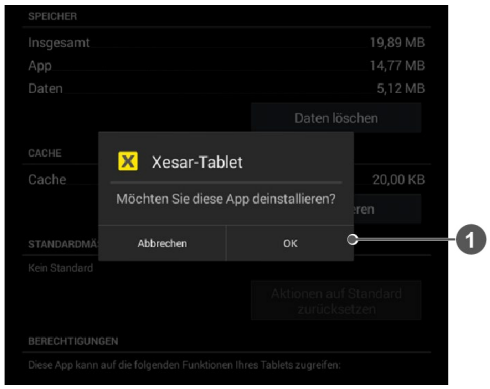
» **2. Schritt:**
Klicken Sie auf Apps ❶.



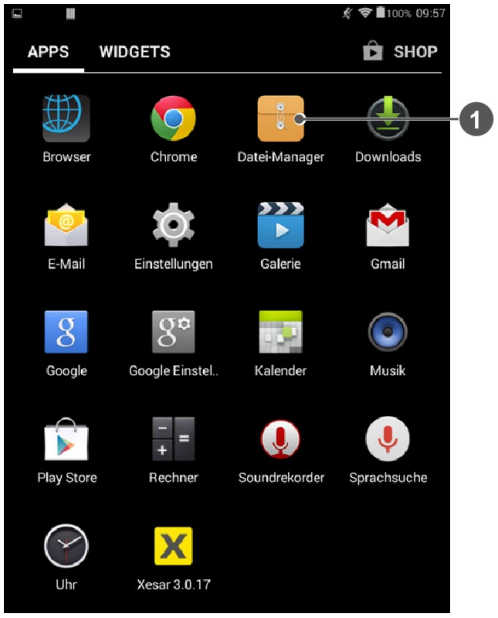
» **3. Schritt:**
Deinstallieren ❶ Sie die Xesar-Wartungsapp.



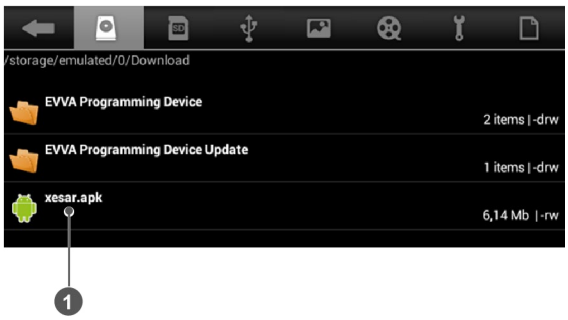
» **4. Schritt:**
Klicken Sie auf OK ❶.



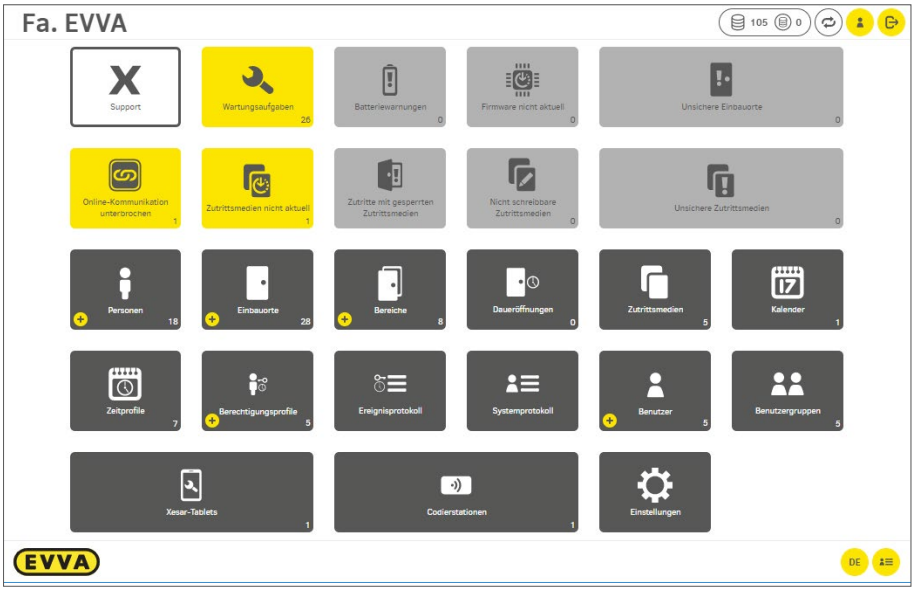
» **5. Schritt:**
Öffnen Sie den Dateimanager Ihres Xesar-Tablets ❶.



» **6. Schritt:**
Klicken Sie auf den Ordner Download und löschen Sie dort die .apk-Datei ❶.

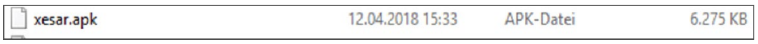


» **7. Schritt:**
Klicken Sie am Xesar-Dashboard auf die Kachel **Support**.

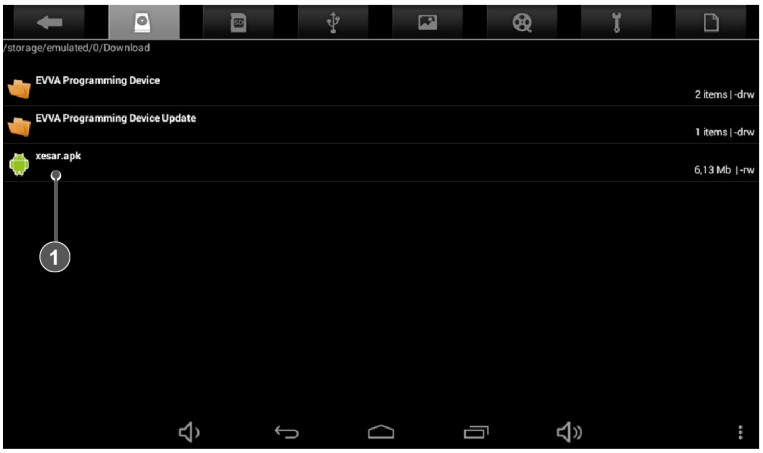


» **8. Schritt:**
Xesar-Tablet herunterladen:
Laden Sie die aktuelle Xesar-Wartungsapp unter **Updates** herunter.
Klicken Sie auf **Xesar-Wartungsapp für Tablet herunterladen** ❶.

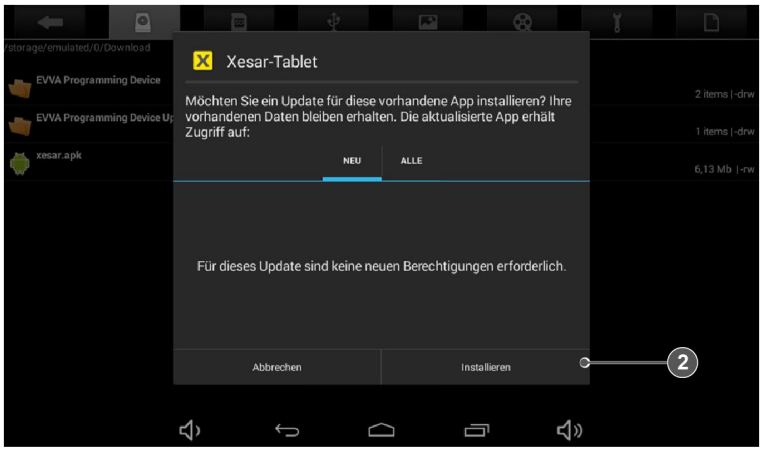
9. Schritt:
Schließen Sie das Xesar-Tablet am USB-Anschluss Ihres Rechner an und ziehen Sie mit der Maus die Datei in den Dateimanager Ihres Xesar-Tablets.



10. Schritt:
Klicken Sie auf die .apk-Datei ❶, um die Xesar-App auf Ihrem Xesar-Tablet zu installieren.



Klicken Sie auf Installieren ❷.



11. Schritt:
Starten Sie die Xesar-Wartungsapp und verbinden Sie das Tablet mit der Xesar-Software. Siehe Kapitel „Tablet mit der Xesar-Software verbinden".

14 Xesar-Anlagen auf PC erstellen

14.1 Installationsvoraussetzungen

Zur Erstellung von Xesar-Anlagen auf PC ist ein Computer mit Windows 10 Pro, Enterprise oder Education erforderlich. In diesen Windows-Versionen ist Hyper-V bereits integriert.

14.2 Hyper-V

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

Hyper-V wird beim Starten des Installation-Managers erkannt und aktiviert.

Hyper-V ist als optionale Funktion in Windows integriert. Es gibt keinen Hyper-V-Download.

» Überprüfen Sie die Anforderungen:
- Windows 10 Enterprise, Pro oder Education
- 64-Bit-Prozessor mit SLAT (Second Level Address Translation)
- CPU-Unterstützung für VM Monitor Mode Extension (VT-c auf Intel-CPUs)
- Mindestens 8 GB RAM, davon 4 GB freier Speicher für die Installation

Die Hyper-V-Funktion kann unter Windows 10 Home nicht installiert werden.

Weitere Informationen und Fehlerbehebung finden Sie unter

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

14.3 Programme für die Erstellung und Verwaltung von Xesar-Anlagen

Zur Erstellung und Verwaltung von Xesar-Anlagen benötigen Sie folgende Programme:

14.3.1 Installation-Manager

Mit dem Installation-Manager verwalten Sie eine oder mehrere Anlagen. Weiters werden Xesar-Systemeinstellungen vorgenommen.

Folgende Aufgaben können durchgeführt werden:

- Einfache Erstellung von Xesar-Anlagen auf PC bzw. Server
- Starten und Stoppen einer Anlage
- Verwaltung der Admin-Karte
- Durchführung von Updates
- Verwaltung von mehreren Anlagen.
- Aufladen von KeyCredits und KeyCredit Xesar-Lifetime
- Einstellen der Backup-Optionen einer Anlage
- Tausch von defekten Admin-Karten
- Einstellen von Anlagen-Ports

14.3.2 Periphery-Manager

Bei Einplatz-Anlagen wird die Codierstation im Installation-Manager verwaltet. Es ist keine zusätzliche Installation des Periphery-Managers notwendig.

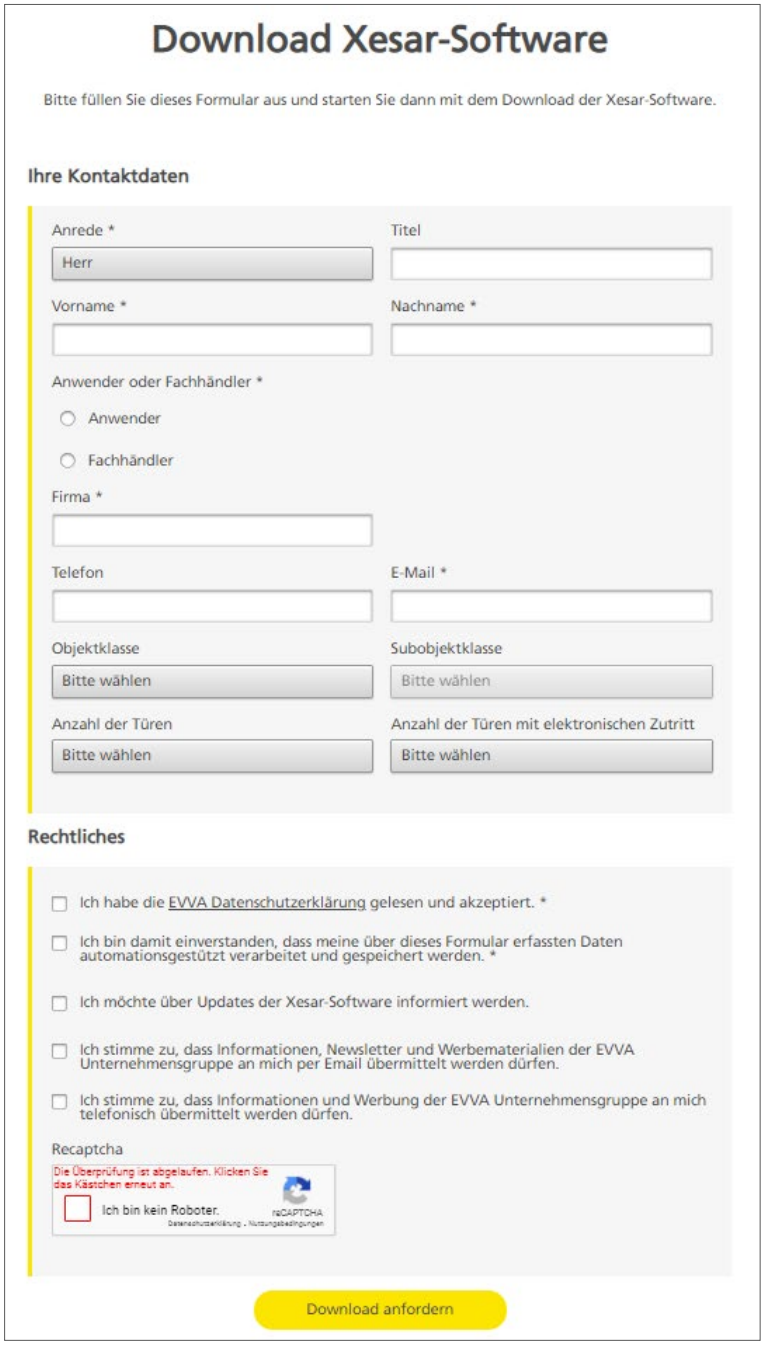
Der Periphery-Manager ermöglicht den Betrieb einer Codierstation an einem Administrator-PC und an Client-PCs bei einer Mehrplatz-Anlage.

Der Periphery-Manager kann in der **Xesar-Software > Support > Updates** heruntergeladen werden.

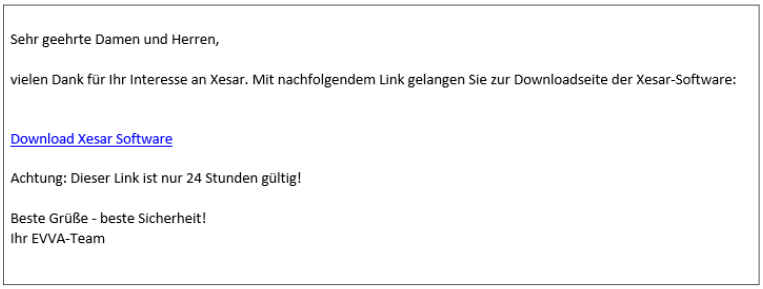
14.3.3 Xesar-Software

Die Xesar-Software ist eine Applikation, die aus dem Installation-Manager aufgerufen wird und in einem Browser läuft. Mit der Xesar-Software kann eine im Installation-Manager gestartete Anlage am Dashboard verwaltet werden.

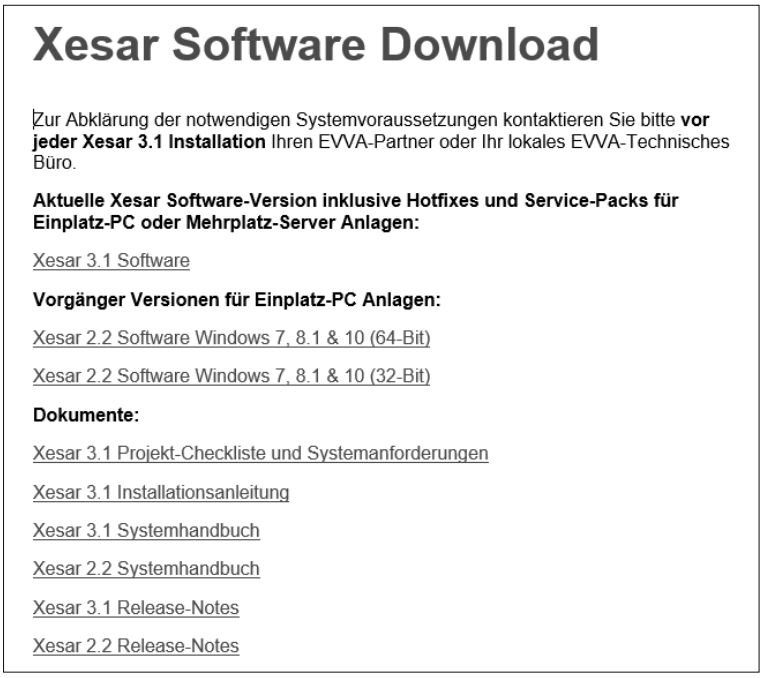
Den Download des aktuellen Installation-Managers finden Sie auf der EVVA-Webseite im Tab Software.



» Füllen Sie das Formular „Download Xesar-Software" aus und senden Sie es ab.



Sie erhalten an die im Formular „Download Xesar-Software" angegebene E-Mail-Adresse eine E-Mail mit einem zeitlich beschränkten Download-Link.



Xesar Software Download

Zur Abklärung der notwendigen Systemvoraussetzungen kontaktieren Sie bitte **vor jeder Xesar 3.1 Installation** Ihren EVVA-Partner oder Ihr lokales EVVA-Technisches Büro.

Aktuelle Xesar Software-Version inklusive Hotfixes und Service-Packs für Einplatz-PC oder Mehrplatz-Server Anlagen:

Xesar 3.1 Software

Vorgänger Versionen für Einplatz-PC Anlagen:

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

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

Dokumente:

Xesar 3.1 Projekt-Checkliste und Systemanforderungen

Xesar 3.1 Installationsanleitung

Xesar 3.1 Systemhandbuch

Xesar 2.2 Systemhandbuch

Xesar 3.1 Release-Notes

Xesar 2.2 Release-Notes

- Laden Sie den aktuellen Installation-Manager herunter.
- Starten Sie die *.msi Datei.

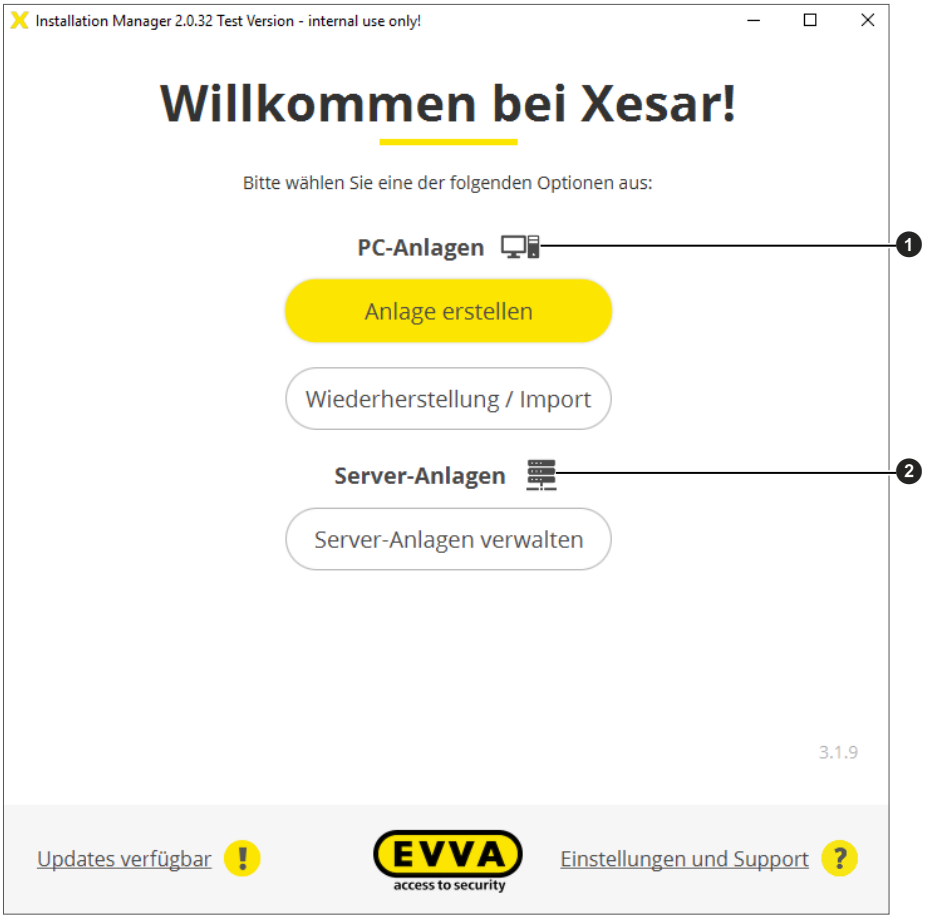
Der Installation-Manager wird automatisch installiert und eine Programm-Verknüpfung im Startmenü und auf dem Desktop erstellt.

- Starten Sie den Installation-Manager mit Klick auf eine der Verknüpfungen.

14.4 Installation-Manager starten

» Starten Sie den Installation-Manager mit Klick auf eine der Verknüpfungen.

Das Startfenster „Willkomen bei Xesar!“ enthält eine Gruppierung in „Xesar-Anlagen auf PC“ ❶ und „Xesar-Anlagen auf Server“ ❷.

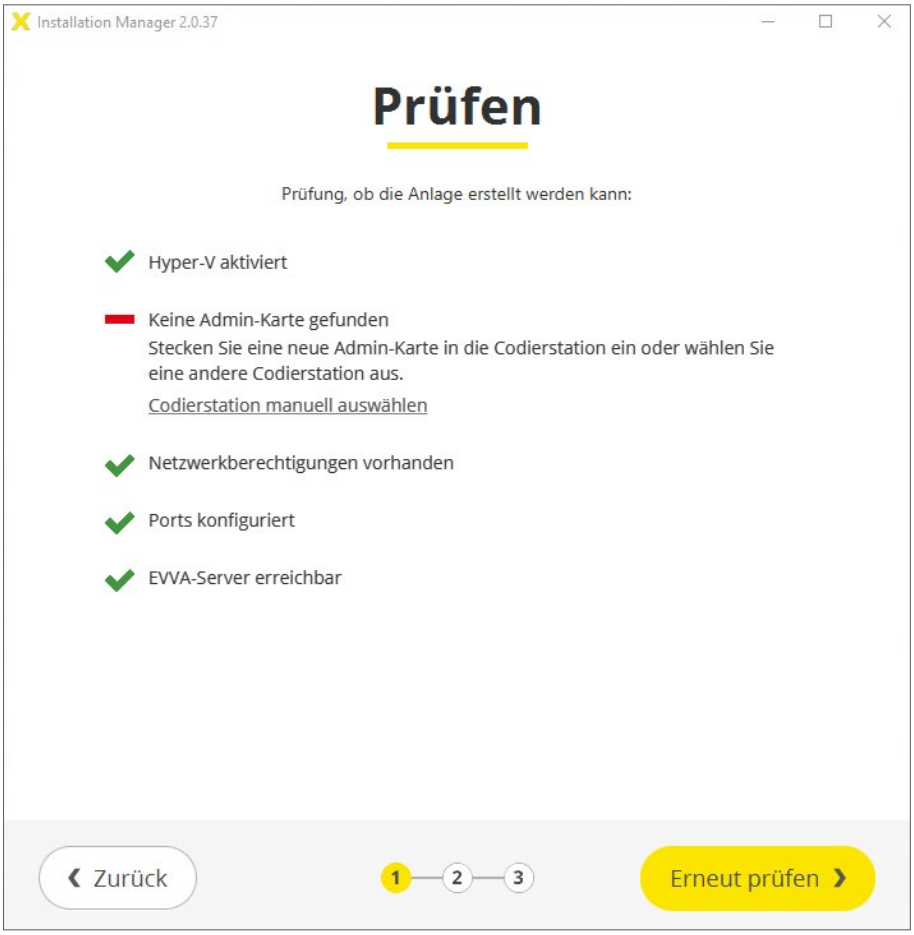


14.4.1 Erstellung einer Xesar-Anlage auf PC

» Klicken Sie auf den Button **Anlage erstellen**, um eine neue Xesar-Anlage auf PC zu erstellen.

Sie werden nun schrittweise durch den Erstellungsvorgang geführt.

» **1. Schritt:**
Prüfung der Voraussetzungen des PCs.



Die zur Verfügung zu stellenden Systemvoraussetzungen entnehmen Sie bitte dem Kapitel „Systemanforderungen“ oder der Projektcheckliste.

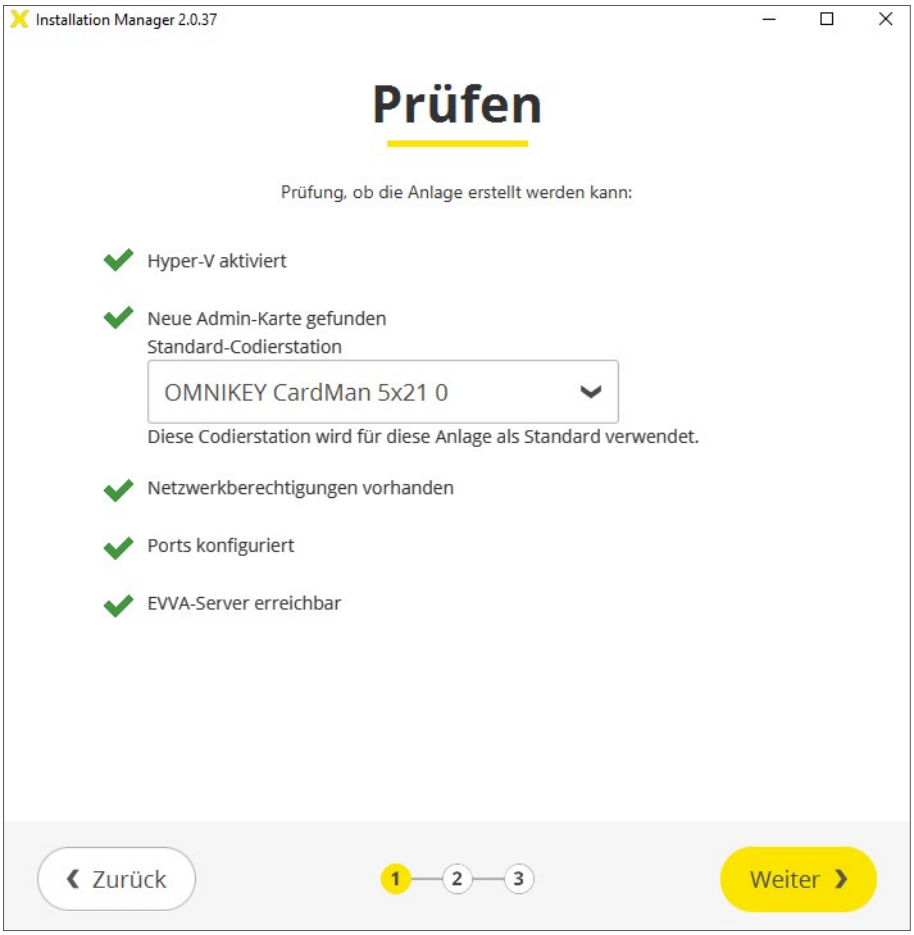
Folgende Anforderungen werden automatisch geprüft:

- Hyper-V ist am PC installiert und aktiviert.
- Eine Codierstation ist angeschlossen und eine neue und gültige Admin-Karte ist eingesteckt.
- Die Netzwerkberechtigung prüft, ob der Installation-Manager auf einem physischen Datenträger und nicht auf einenem Netzlaufwerk installiert wurde.
- Die von Xesar benötigten Ports sind frei und verfügbar.
- Der EVVA-Server ist über das Internet erreichbar. Dies ist notwendig, um z. B. die Liste der verfügbaren Updates zu überprüfen.

Wenn nicht alle zur Installation nötigen Anforderungen erfüllt sind, werden Fehlermeldungen mit Lösungsvorschlägen angezeigt.

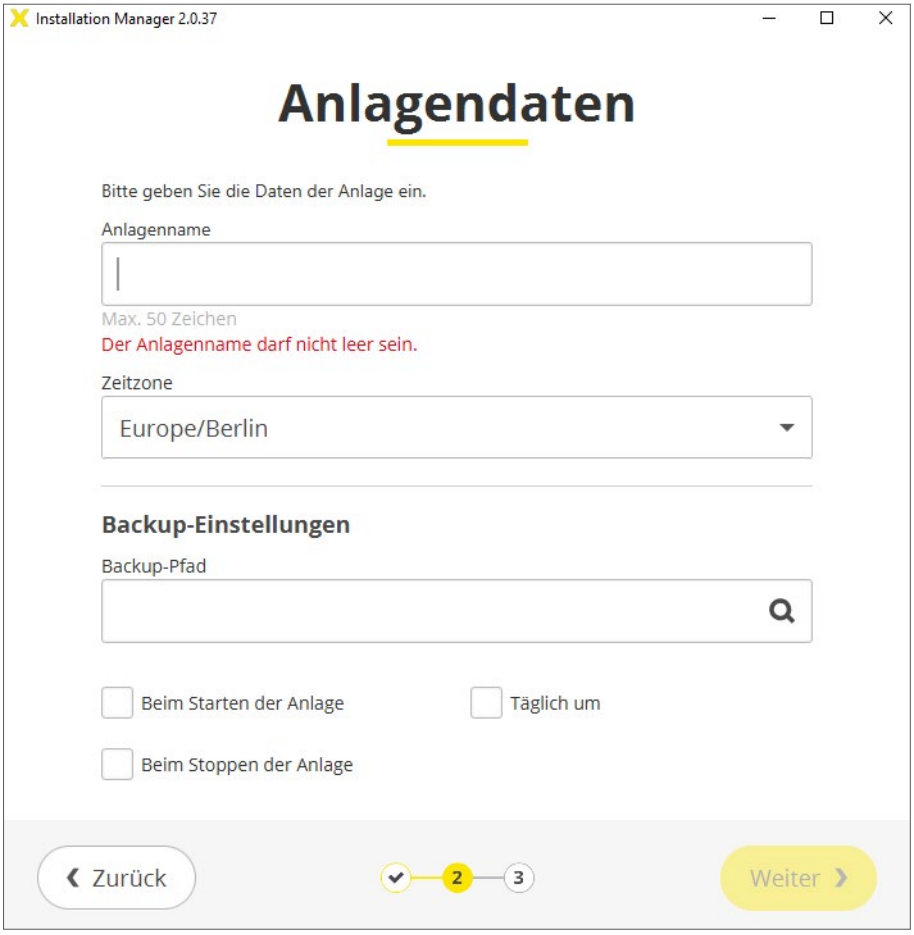
» Versuchen Sie, das Problem laut Hinweis zu lösen und klicken Sie auf **Erneut prüfen**.

Lässt sich das Problem nicht lösen, wenden Sie sich bitte an Ihren EVVA-Partner oder an das Technische Büro von EVVA.

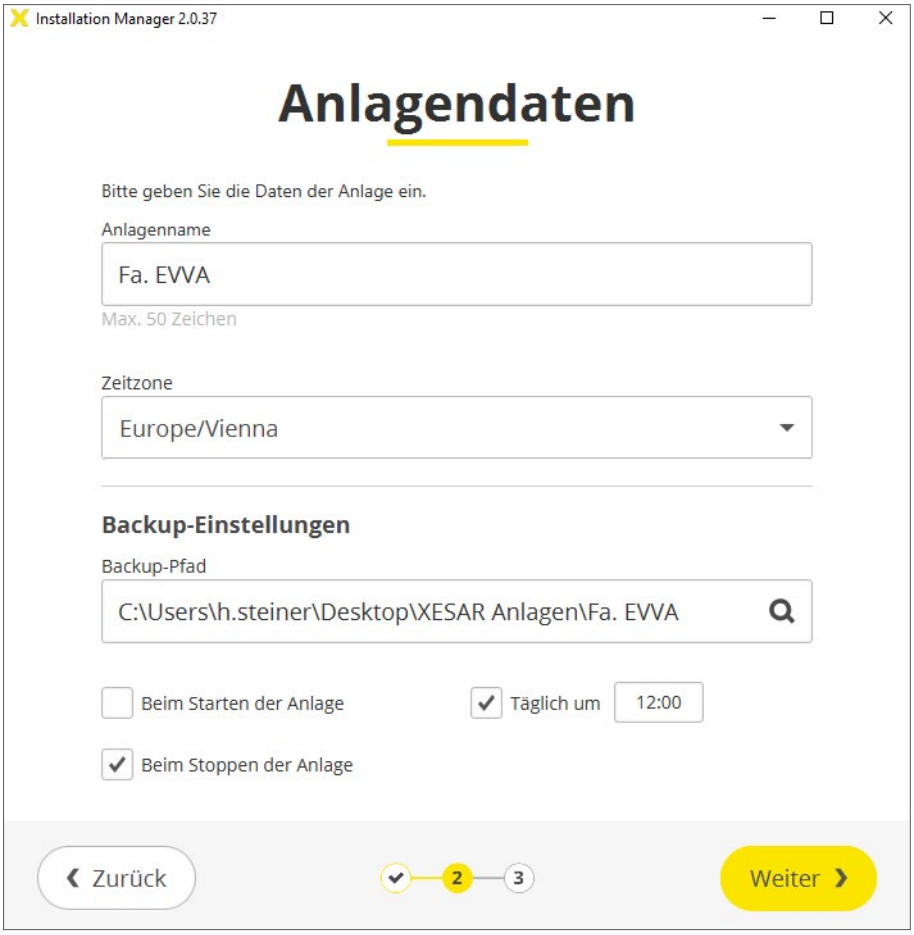


Wenn alle Anforderungen erfolgreich geprüft sind, klicken Sie auf **Weiter**, um den Vorgang fortzusetzen.

» **2. Schritt:**
Fügen Sie die Anlagendaten und die gewünschten Backup-Einstellungen in die vorgegebenen Felder ein.

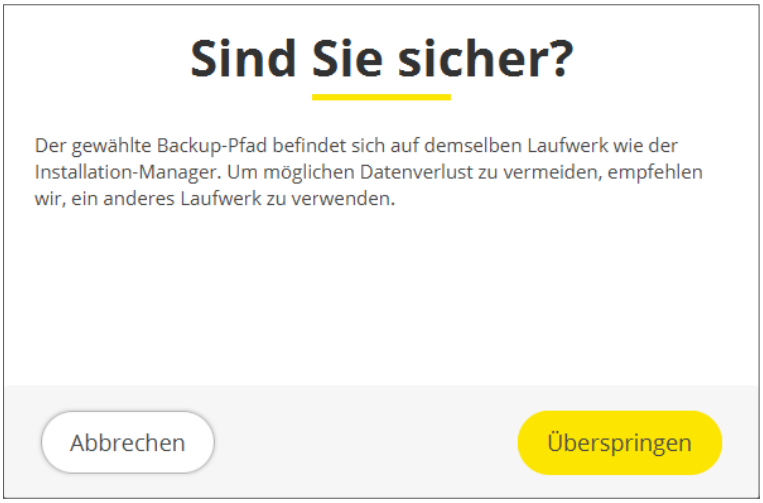


Die Auswahl mehrerer Backup-Optionen ist möglich.



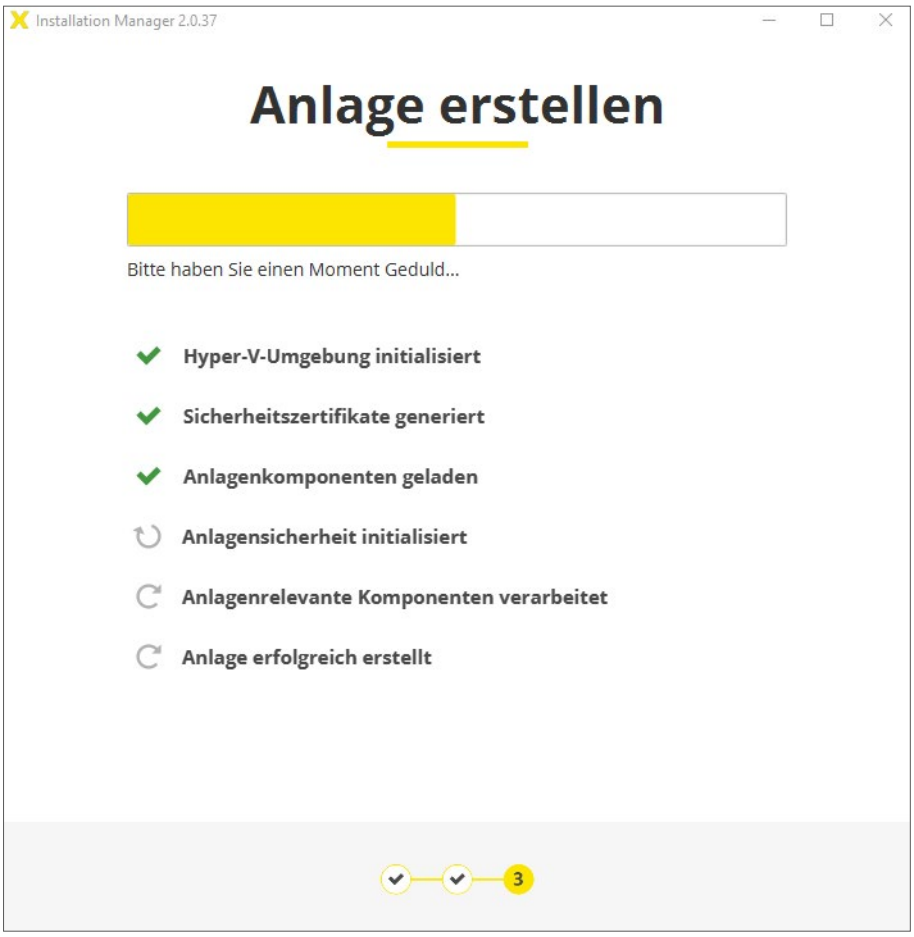
Um Datenverluste bei einem Hardwareproblem zu vermeiden, sollen Backup-Daten nicht auf gemeinsamen Laufwerken der Xesar-Software gespeichert werden.

Wenn Sie den Backup-Pfad auf dem Laufwerk des Installation-Managers auswählen, erscheint der Hinweis „Sind Sie sicher?".

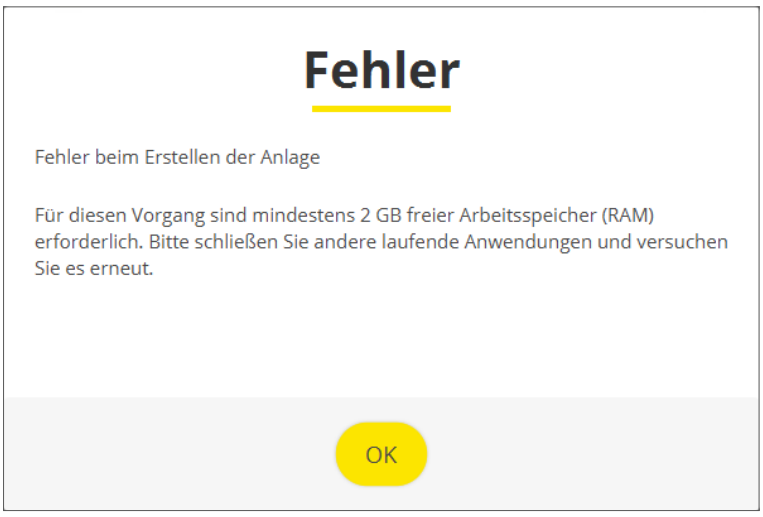


Klicken Sie auf **Abbrechen,** kommen Sie zurück und können einen neuen Backup-Pfad angeben. Durch Klicken auf **Überspringen** ignorieren Sie die Warnung.

» **3. Schritt:**
Erstellen der Anlage



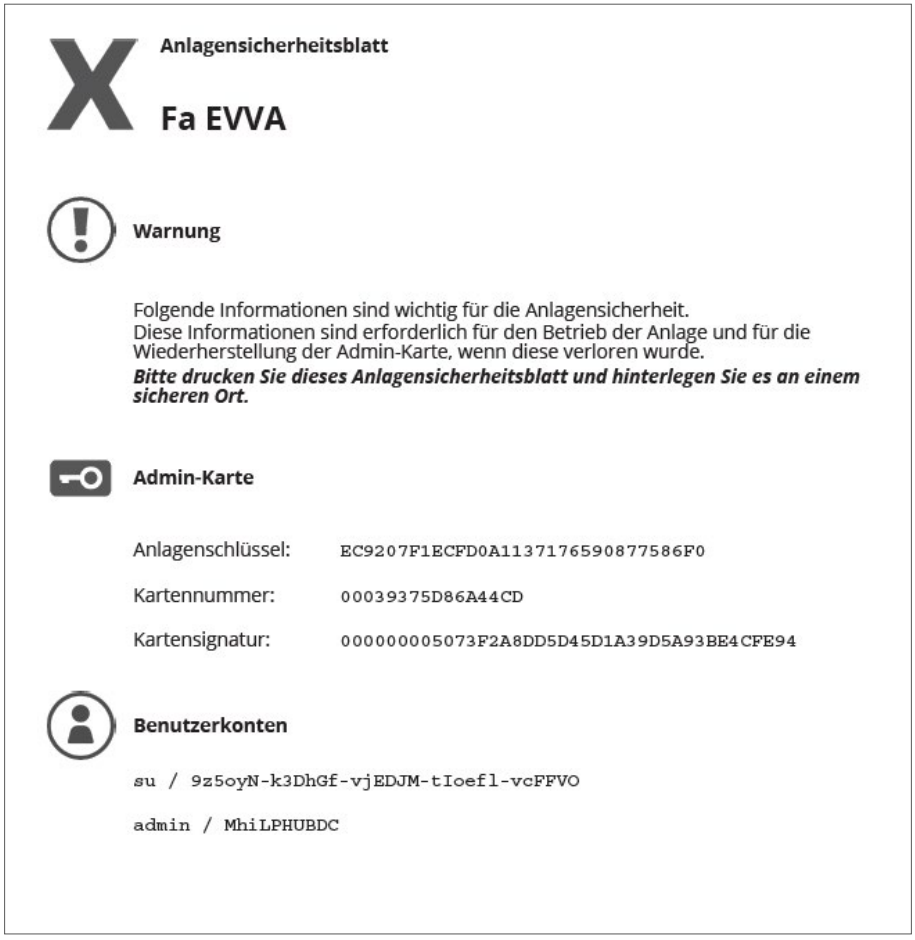
Folgende Fehlermeldung erscheint, wenn während des Installationsvorgangs zu wenig freier Arbeitsspeicher (mind. 2 GB) vorhanden ist.



14.4.2 Anlagensicherheitsblatt

Nach erfolgreicher Installation der Anlage wird das Anlagensicherheitsblatt mit den wichtigen Anlageninformationen generiert und automatisch als PDF angezeigt.

Darauf befinden sich die Benutzer-Passwörter zum Anmelden des Systemadministrators (su) und des Administrators (admin).



Anlagensicherheitsblatt

Fa EVVA

Warnung

Folgende Informationen sind wichtig für die Anlagensicherheit.
Diese Informationen sind erforderlich für den Betrieb der Anlage und für die Wiederherstellung der Admin-Karte, wenn diese verloren wurde.
Bitte drucken Sie dieses Anlagensicherheitsblatt und hinterlegen Sie es an einem sicheren Ort.

Admin-Karte

Anlagenschlüssel:	EC9207F1ECFD0A1137176590877586F0
Kartennummer:	00039375D86A44CD
Kartensignatur:	000000005073F2A8DD5D45D1A39D5A93BE4CFE94

Benutzerkonten

su / 9z5oyN-k3DhGf-vjEDJM-tIoefl-vcFFVO

admin / MhiLPHUBDC

Sie können das Anlagensicherheitsblatt auch durch Klicken auf den Button **Anlagensicherheitsblatt öffnen (PDF)** öffnen.

Drucken Sie das Anlagensicherheitsblatt aus. Bestätigen hier den Ausdruck und verwahren Sie den Ausdruck an einem sicheren Ort.

Bei Verlust oder Defekt der Admin-Karte sind die Informationen des Anlagensicherheitsblattes die einzige Möglichkeit, die Anlage weiter zu betreiben.

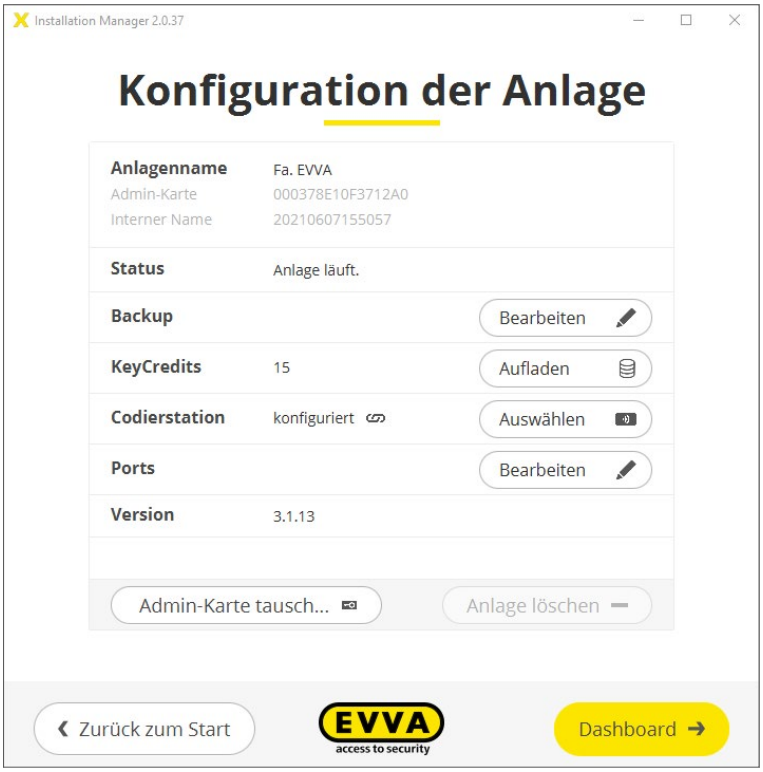
EVVA kann keine Wiederherstellung der Daten durchführen, wenn das Anlagensicherheitsblatt mit den Informationen der Anlage fehlt!

» Klicken Sie auf **Weiter**, um die Anlage zu starten.
(Es kann einige Minuten dauern, bis die Anlage gestartet ist.)

- Klicken Sie auf den Button **Dashboard** – Sie kommen zum Login der Anlagenverwaltung

- Klicken Sie auf den Button **Konfigurieren** – Sie kommen zur Konfigurationsseite der Anlage.

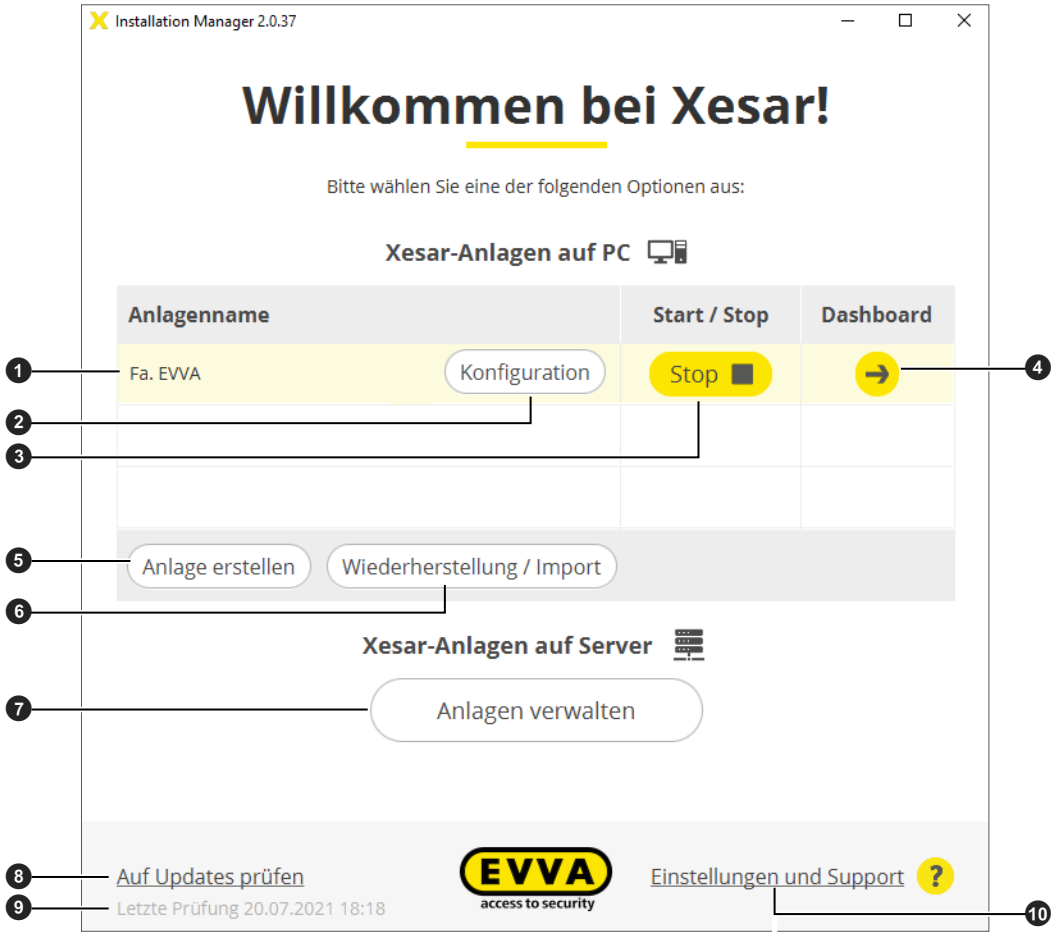
Hier sehen Sie im Überblick alle wichtigen Anlageneinstellungen.
Bei Bedarf können anlagenrelevante Änderungen vorgenommen werden.



Damit ist die Installation der Anlage abgeschlossen.

» Klicken Sie auf den Button **Zurück zum Start** – Sie kommen auf die Startseite des Installation-Managers.

15 Startseite Installation-Manager



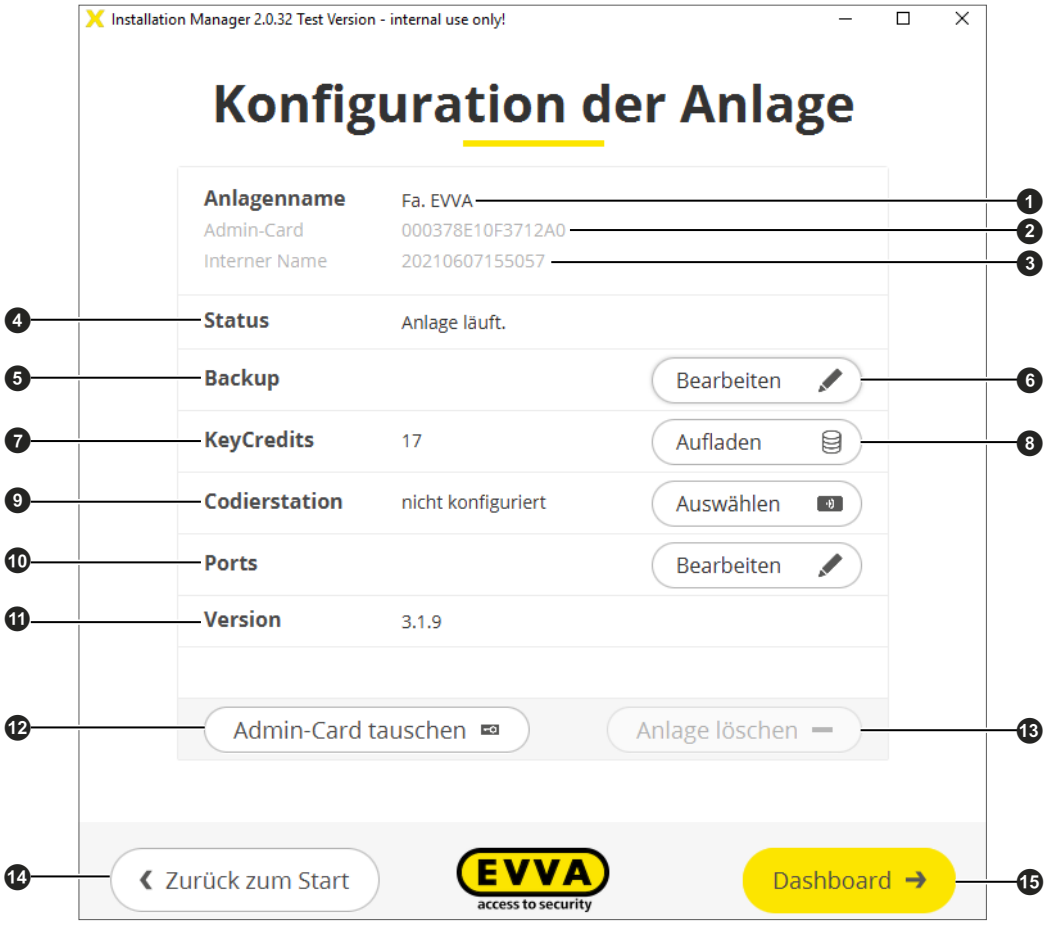
Funktionen der Installation-Manager-Startseite:

- Anzeige der Version des Installation-Managers
- PC- Anlagen:
  - Anlagename ❶
  - Button **Konfiguration** ❷ zur Anlagen-Konfigurationsseite.
  - Button **Start/Stop** ❸ zum Starten bzw. Stoppen der ausgewählten Anlage.
  - Button **Dashboard** ❹ zur Login-Seite der Anlage
  - Button **Anlage erstellen** ❺ startet den Installationsablauf für eine neue Anlage.
  - Button **Wiederherstellung/Import** ❻: Anlagenwiederherstellung mit Back-up-Datei oder Upgrade einer Xesar 2.2 Bestandsanlage.
- Xesar-Anlagen auf Server:
  - Button zur Ansicht der Xesar-Anlagen auf Server und Xesar-3.0-Anlagen nach Update auf 3.1 (Siehe Kapitel „Xesar-Anlagen auf Server“) ❼.
- Button **Update prüfen**: Überprüfen nach Updates von Installation-Manager und Xesar-Software. Bei Vorhandensein eines Updates wird dieses angezeigt ❽. Mit Klick auf den Button gelangen Sie zur Update-Seite.

- Datum der letzten Update-Überprüfung ❾.

- Einstellungen und Support ❿ (nur für PC- Anlagen):
  - Autostart: Das automatische Starten des Installation-Managers nach dem Hochfahren des PCs kann aktiviert bzw. deaktiviert werden.
  - Proxy-Einstellungen: Bei Bedarf können hier Proxy-Einstellungen vorgenommen werden.
  - Support-Informationen: Generierung einer Datendatei zur besseren Fehleranalyse durch den EVVA-Support im Fehlerfall.

15.1 Konfiguration der Anlage

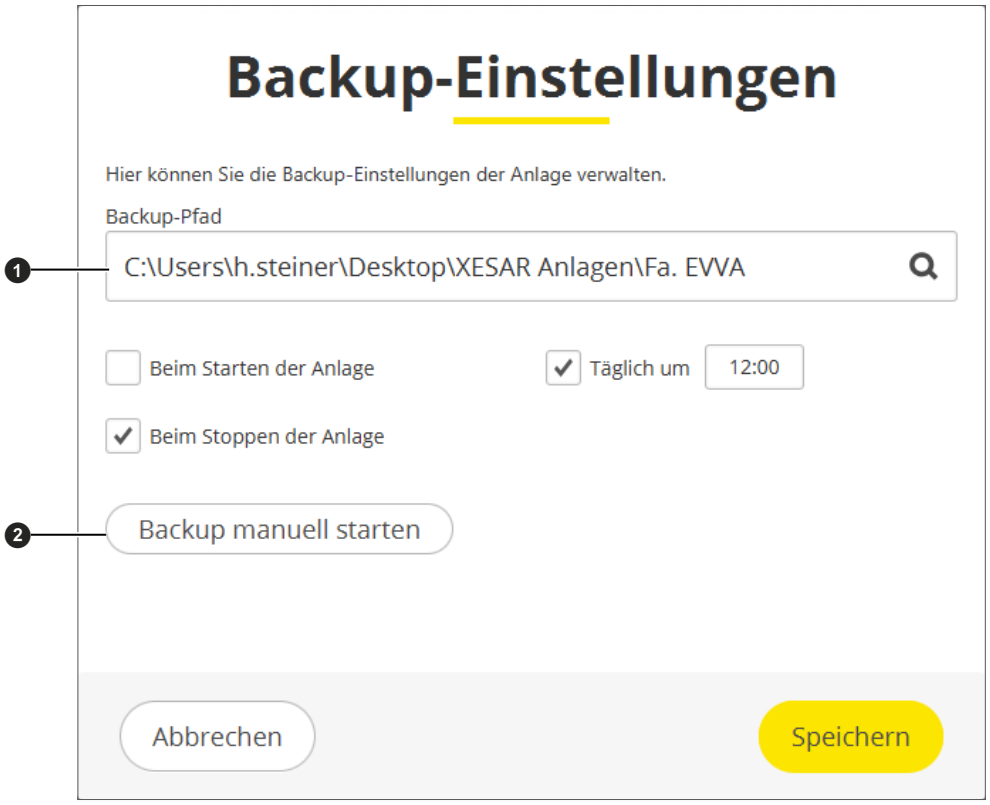


Funktionen der Anlagen-Konfigurationsseite:

- Anlagenname ❶
- Admin Card ❷: Nummer der Admin-Karte
- Interne Nummer der Anlage ❸
- Status der Anlage ❹:
  - Anlage läuft
  - Anlage gestoppt

- Backup ❺:
  - Datum des letzten Backups
  - Button **Einrichten** ❻ zum Einrichten des Zeitpunktes des Anlagen-Backup.
- KeyCredits ❼:
  - Anzahl der verfügbaren Stück KeyCredits oder Ansicht Lifetime-Symbol ∞.
  - Button **Aufladen** ❽ zum KeyCredits Aufladen.
- Codierstation ❾: Auswahl der Codierstation zur Zutrittsmedienverwaltung
- Ports ❿: Einstellen der Ports, wenn die Standard Ports belegt sind (nur bei gestoppter Anlage möglich).
- Xesar-Software Version ⓫
  - Button **Admincard tauschen** ⓬: Tausch bei defekter Admin-Karte.
  - Button **Anlage löschen** ⓭: Löschen einer Xesar-Anlage auf PC (nur bei gestoppter Anlage möglich).
  - Button **Zurück zum Start** ⓮: Zurück zur Installation-Manager-Startseite.
  - Button **Dashboard** ⓯: Zur Anmeldung der Anlage im Browser.

15.1.1 Backup-Einstellungen



- Backup-Pfad ❶:
  - » Geben Sie den gewünschten Pfad für die Backups Ihrer Anlage ein.

!	Das Laufwerk soll nicht identisch mit dem Anlagen-Laufwerk sein.

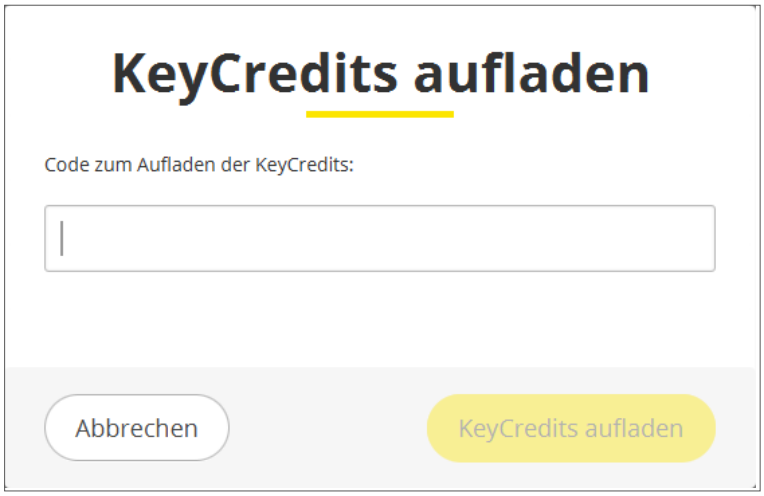
- Einstellmöglichkeit für automatische Backups:
  - Backup beim Starten der Anlage.
  - Backup beim Stoppen der Anlage (empfohlen).
  - Backup – täglich zu definierter Uhrzeit.
- Button **Backup manuell starten ❷**: Manuelles Backup ist jederzeit möglich.

Die Backup-Dateien finden Sie unter dem angegebenen Backup-Pfad.

15.1.2 KeyCredits aufladen

Für die Erstellung und Änderungen von Zutrittsberechtigungen von Zutrittsmedien werden KeyCredits verrechnet.

Für die Verwaltung von Anlagen stehen 2 Lizenzmodelle zur Verfügung:
- Xesar Stück KeyCredits
- KeyCredit Xesar-Lifetime



» Geben Sie den Code zum Aufladen der KeyCredits in das Eingabefeld ein und klicken Sie auf **KeyCredits aufladen**.

Bei Stück KeyCredits erhöht sich das Guthaben auf der Konfigurationsseite im Installation-Manager bzw. am Dashboard der Anlage um den entsprechenden Wert. Von diesem Guthaben werden die für Berechtigungserstellung und Änderungen verwendeten KeyCredits abgebucht.

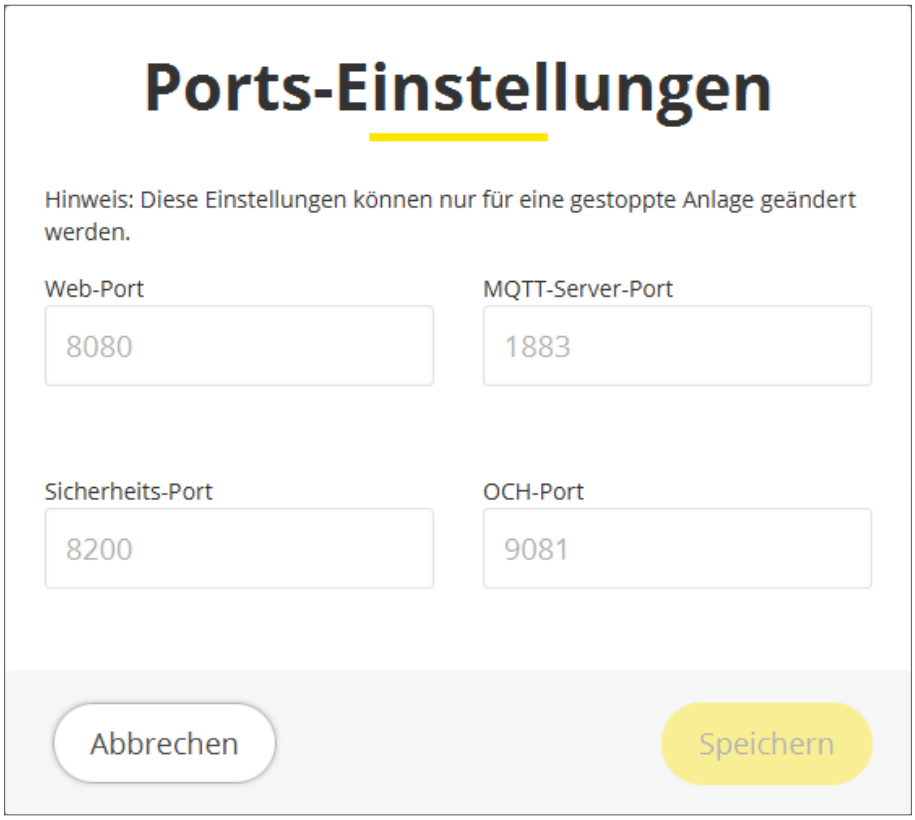
Bei KeyCredits Xesar-Lifetime wird das Lifetime-Symbol angezeigt. Für die Berechtigungserstellung und Änderungen werden keine weiteren KeyCredits benötigt.

Zum Aufladen von KeyCredits muss die Anlage gestartet und mit dem EVVA-Server über das Internet verbunden sein.

15.1.3 Ports-Einstellungen (manuell einrichten)

Bei der Erstellung der Anlage werden die für Xesar benötigten Standard-Ports automatisch eingerichtet. Sind diese Ports im Anlagennetzwerk nicht frei, können hier die Ports manuell eingetragen werden.

Zum manuellen Einrichten der Ports muss die Anlage gestoppt werden.

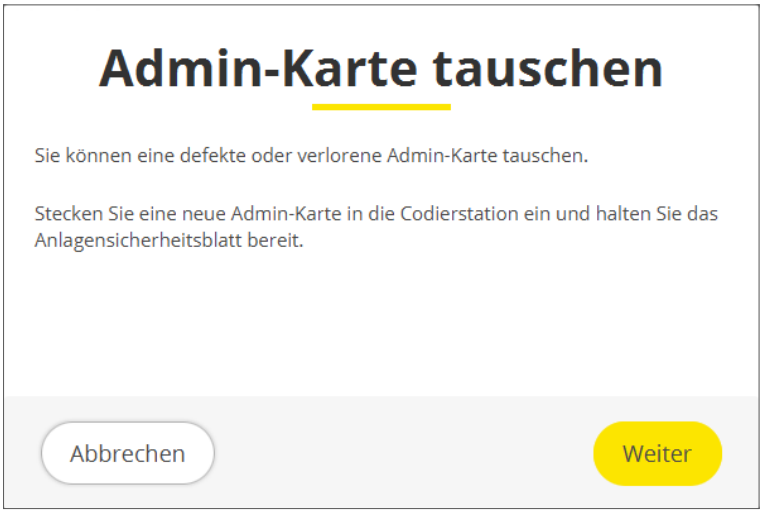


» Geben Sie die Port Adressen in die Eingabefelder ein und klicken Sie auf **Speichern**.

15.1.4 Admin-Karte tauschen

Bei Defekt oder Verlust der Admin-Karte der Anlage kann sie gegen eine neue Admin-Karte getauscht werden.

» Klicken Sie dazu in der Konfigurationsseite auf **Admin-Karte tauschen** und folgen Sie den Anweisungen.



15.1.5 Anlage löschen

» Um eine Anlage zu löschen, klicken Sie auf **Löschen**.

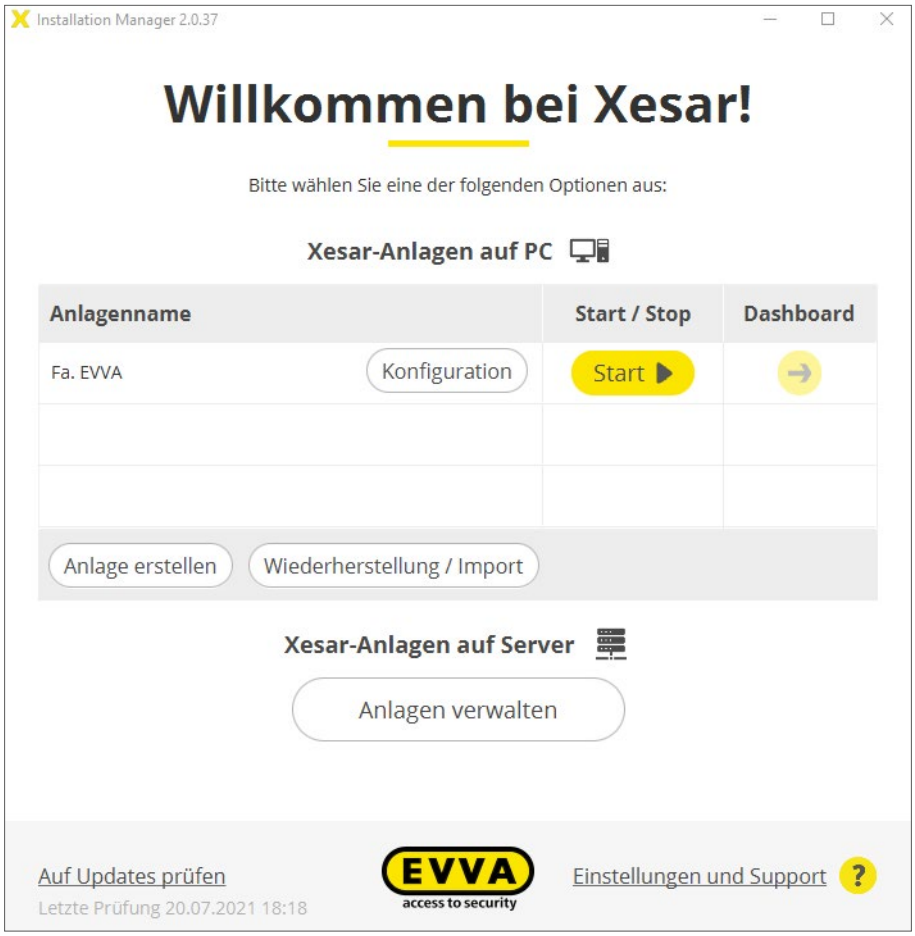
Vor dem Löschen muss die Anlage gestoppt werden.

15.2 Starten einer bestehenden Anlage

» Starten Sie den Installation-Manager durch Klick auf das Icon am Desktop.

Der Installation-Manager führt eine automatische Systemprüfung durch, ob alle für den Start der Anlage notwendigen Anforderungen erfüllt sind.

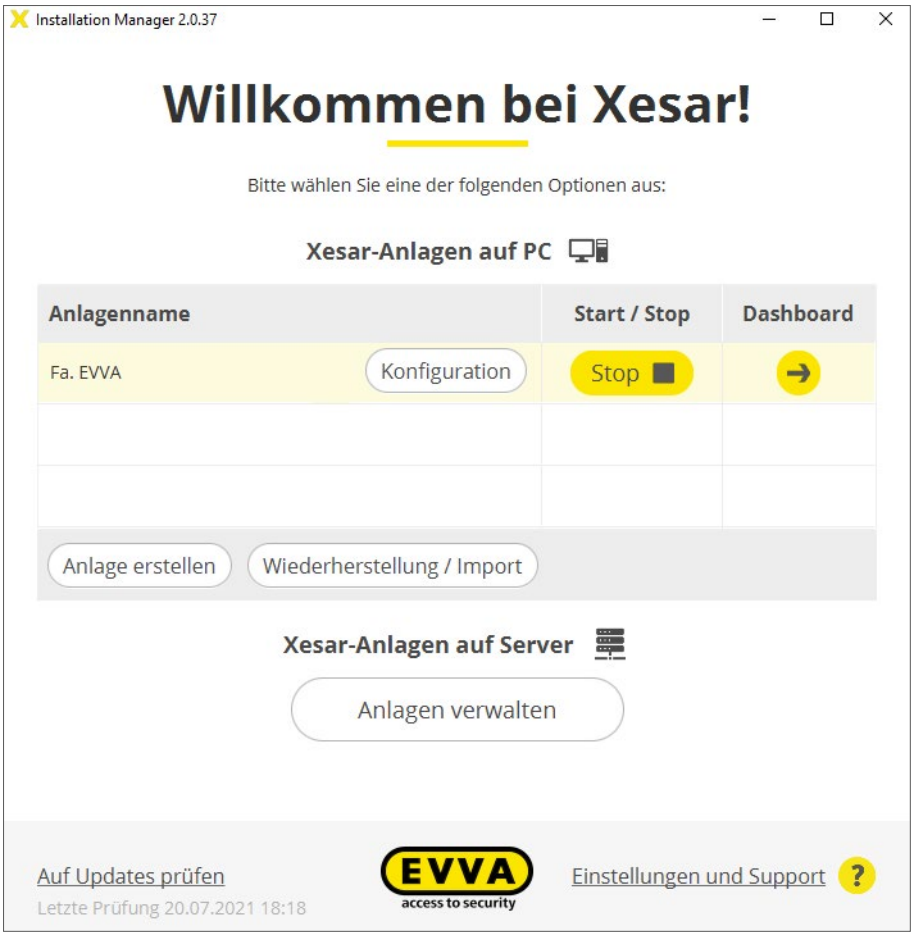
15.2.1 Starten der Anlage mit eingelegter Admin-Karte



» Starten Sie die Anlage mit Klick auf den Start-Button.

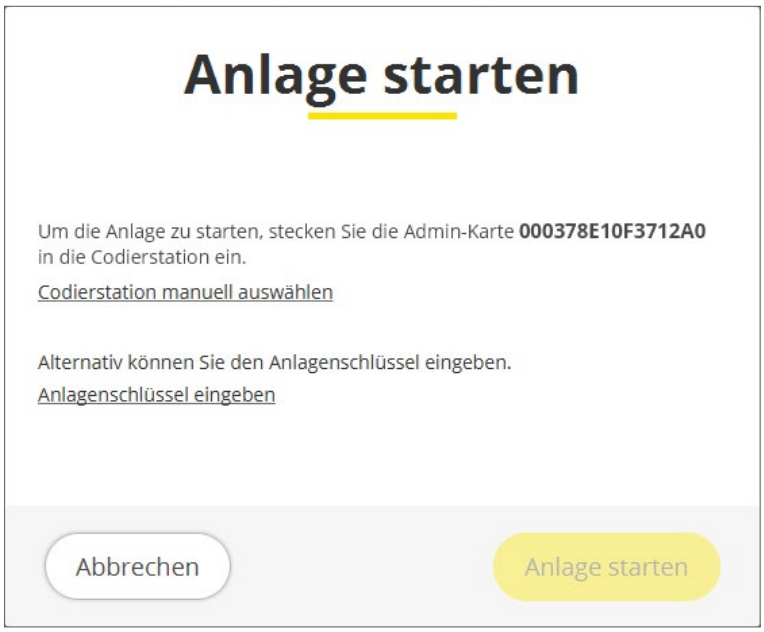
Es folgt die Prüfung der Admin-Karte. Ist die richtige Admin-Karte eingelegt, wird die Anlage gestartet.

» Nach erfolgreichem Anlagenstart drücken Se den Button **Dashboard**, um zum Login der Anlagenverwaltung zu kommen.



15.2.2 Starten der Anlage ohne Admin-Karte

Wenn keine oder eine für die Anlage falsche Admin-Karte steckt, wird folgende Fehlermeldung angezeigt:



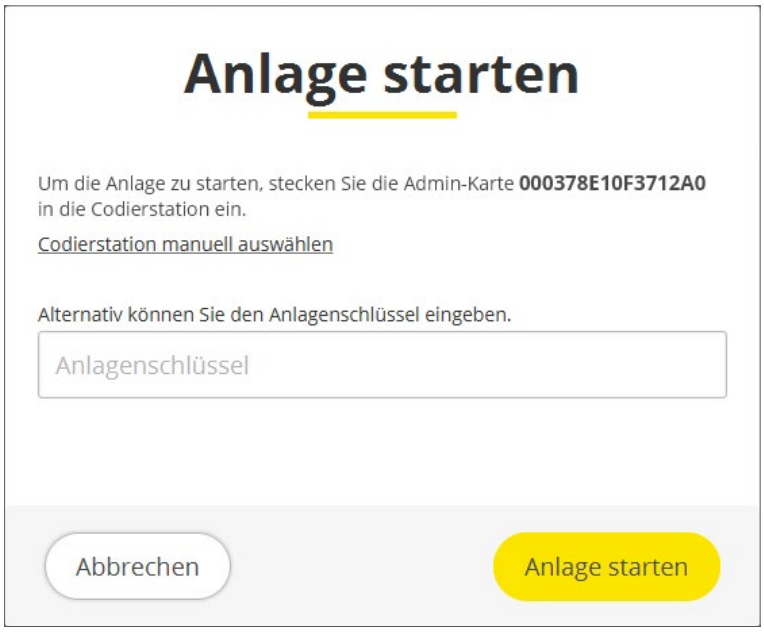
» Stecken Sie die richtige Admin-Karte mit der entsprechenden Admin-Kartennummer in die Codierstation und
» starten Sie die Anlage.

Oder alternativ

» Geben Sie den Anlagenschlüssel ein und
» starten Sie die Anlage.

Den Anlagenschlüssel finden Sie auf dem Anlagensicherheitsblatt.

Die Anlage kann nur mit dem Anlagenschlüssel gestartet werden. Änderungen auf der Konfigurationsseite der Anlage können nur mit eingesteckter Admin-Karte durchgeführt werden.



15.3 Einstellungen und Support

Die unter „Einstellungen und Support" vorgenommenen Einstellungen gelten nur für Xesar-Anlagen auf PC.

15.3.1 Autostart

Bei aktivierter Autostart-Funktion werden der Installation-Manager und die laufende Anlage nach einem PC-Neustart wieder automatisch gestartet.

Aktivieren Sie Autostart, wenn Sie in Ihrer Xesar-Anlage auf PC Online-Wandleser betreiben.

15.3.2 Proxy-Einstellungen

Unter Proxy-Einstellungen können bei Bedarf die entsprechenden Einstellungen vorgenommen werden.

- Proxy-Server verwenden ❶ aktivieren oder deaktivieren
- DNS-Name / IP-Adresse ❷ des Proxy-Servers
- Port ❸: Proxy-Server Port
- Benutzername ❹: Proxy-Server Benutzername
- Passwort ❺: Proxy-Server Benutzerpasswort

15.4 Wiederherstellung/Import

Folgende Situationen benötigen eine Wiederherstellung oder den Import einer Anlage:

- Wiederherstellung nach einem Hard- oder Software-Fehler.
- Transfer auf eine neue Hardware.
- Upgrade einer älteren Anlage.

Für ein Upgrade oder den Transfer der Anlage ist es wichtig, dass Sie **vor Wiederherstellung/Import eine aktuelle Backup-Datei erzeugen**. Das Backup kann mit der Durchführung eines manuellen Backups erfolgen.

Eine wiederherzustellende Anlage darf NICHT bereits im Installation-Manager vorhanden sein.

Zur erfolgreichen Wiederherstellung/Import einer Anlage sind folgende Komponenten notwendig:

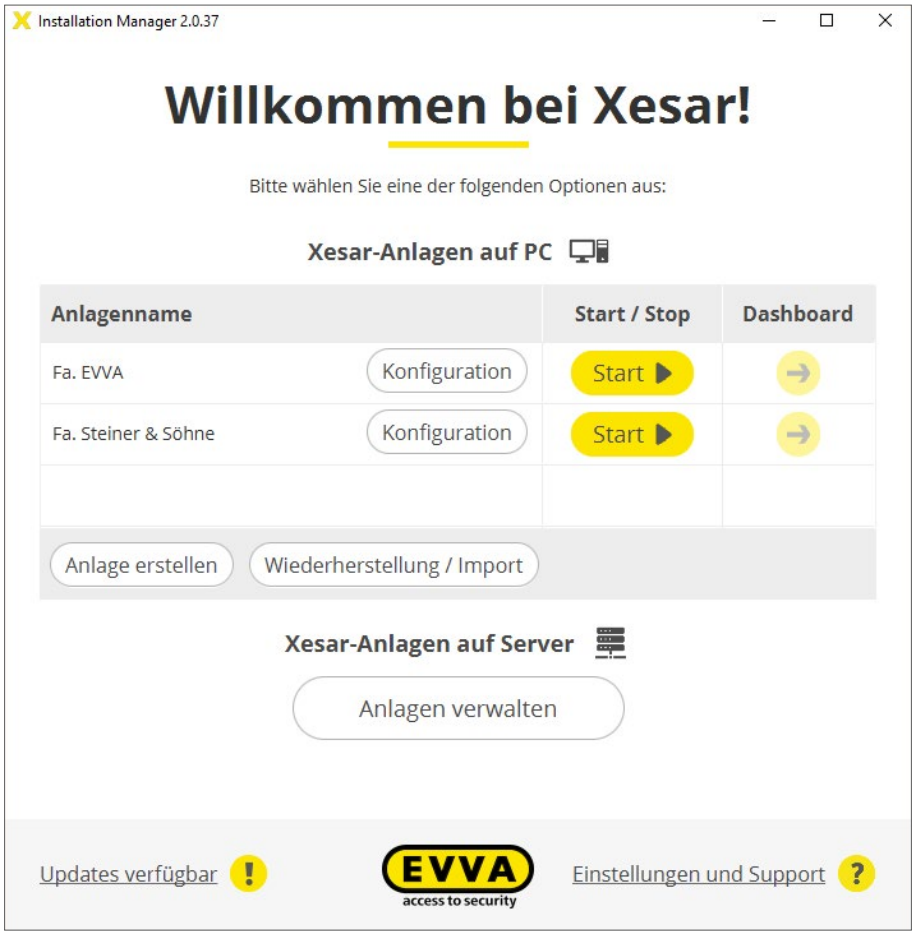
- Eine möglichst aktuelle Backup-Datei der Anlage.
- Die Admin-Karte der zu importierenden Anlage muss in der Codierstation eingesteckt sein.
- Alle Anlagen im Installation-Manager müssen gestoppt sein.

» Wählen Sie die zur Wiederherstellung oder zum Import notwendige Backup-Datei.
» Klicken Sie auf **Importieren** und folgen Sie den Anweisungen.

15.5 Update von Installation-Manager und Anlagen

Der Installation-Manager und die Anlagen werden getrennt aktualisiert.

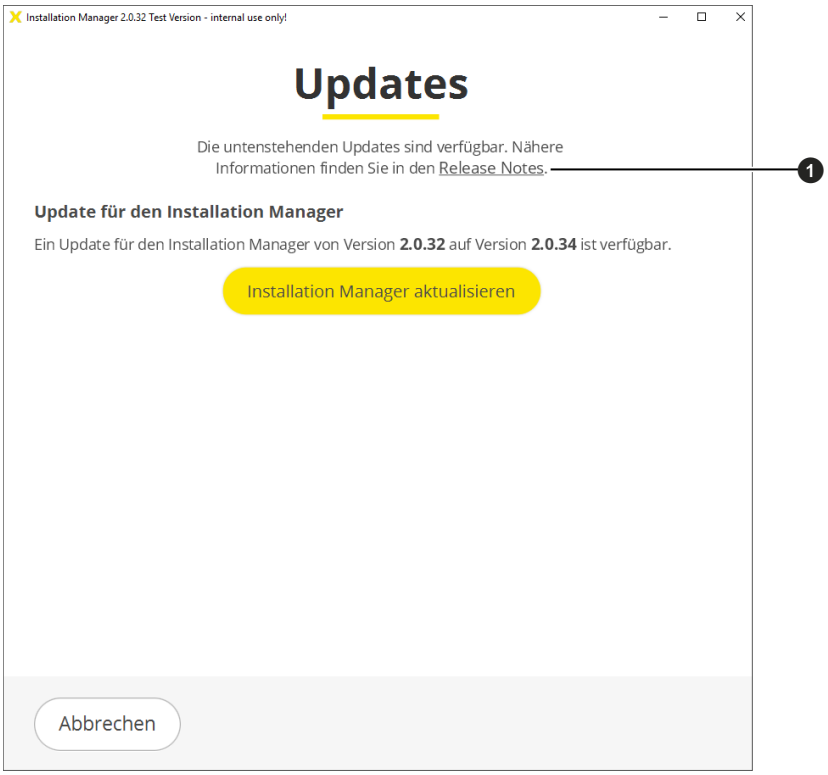
Die Updates von Installation-Manager und der Anlage werden im Installation-Manager durchgeführt.



Updates verfügbar : Bei vorhandenen Updates wird der Hinweis hervorgehoben angezeigt.

» Klicken Sie auf **Updates verfügbar**, wird die Seite mit den möglichen Updates angezeigt.

» Folgen Sie zum Durchführen der Updates den Anweisungen



Auf der Updates-Seite werden alle verfügbaren Updates für den Installation-Manager und die vorhandenen Anlagen angezeigt.

Der Link „Release Notes" ❶ führt Sie zu den Release Notes mit den beschriebenen Neuerungen der Update-Versionen.

» Führen Sie zuerst das Update des Installation-Managers aus.
» Anschließend führen Sie das Update für die jeweilige Anlage aus.

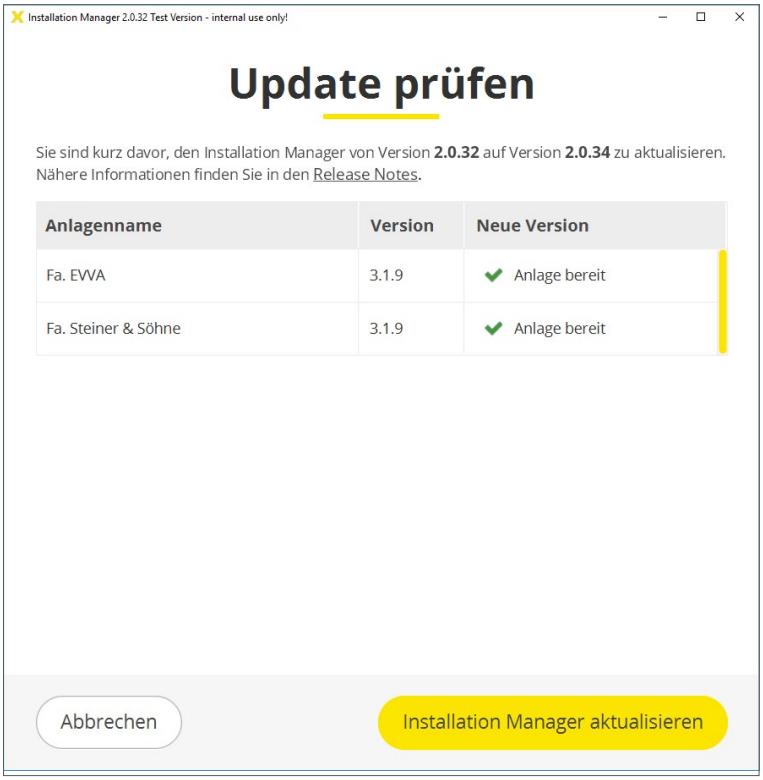
Update prüfen: Wenn keine Updates angezeigt werden, überprüfen Sie mit Klick auf den Link, ob neue Updates verfügbar sind.

Das Datum der letzten Update-Überprüfung ❷ wird angezeigt.

Um Updates empfangen zu können, muss der Anlagen-PC über das Internet mit dem EVVA-Server verbunden sein.

15.5.1 Installation-Manager aktualisieren

» Klicken Sie auf der Seite „Updates“ auf den Button **Installation-Manager aktualisieren**.



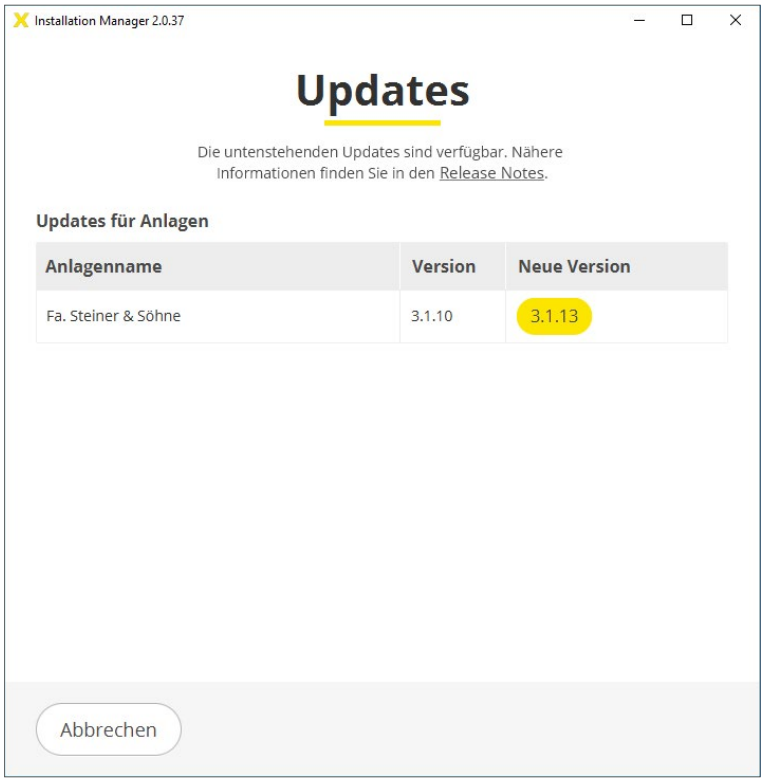
Vor dem Update des Installation-Managers wird überprüft, ob die vorhandene Anlage auf Grund ihrer Version mit dem neuen Installation-Manager aktualisiert werden kann.

Wenn die Anlage für das Update des Installation-Managers bereit ist, wird das in der Spalte „Neue Version“ angezeigt.

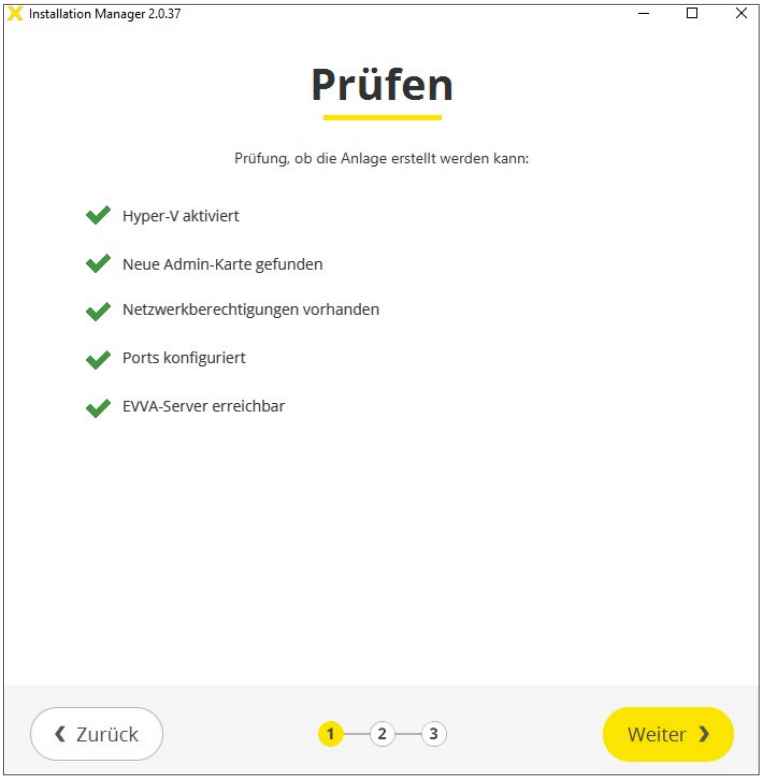
» Klicken Sie auf den Button **Installation-Manager aktualisieren**.

15.5.2 Update von Anlagen

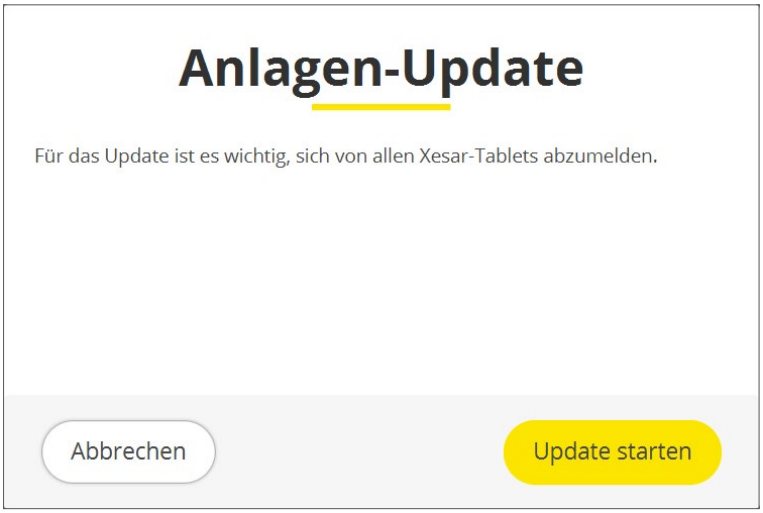
Anlagen-Updates werden auf der Anlagenseite in der Spalte „Neue Version“ angezeigt.



» Klicken Sie auf den jeweiligen Versions-Button.



Vor dem Update werden alle notwendigen Anforderungen und Einstellungen überprüft.

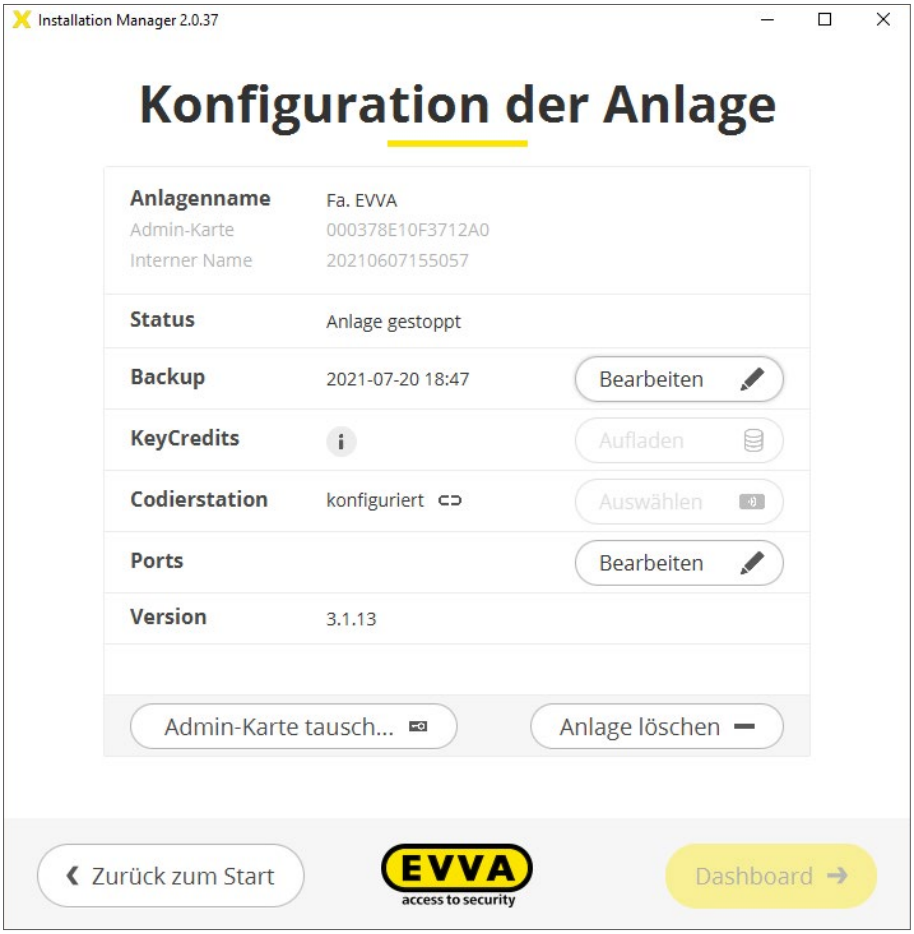


» Wenn alle Anforderungen erfüllt sind, klicken Sie auf **Update starten** und folgen Sie den Anweisungen.

Vor dem Update der Anlage müssen alle in der Anlage angemeldeten Tablets durch ein Logout am jeweiligen Tablet abgemeldet werden.

Vor dem Update der Anlage wird ein Backup gemacht. Dazu muss die Anlage gestartet werden.

» Klicken Sie auf **Update starten**, wird die Anlage aktualisiert.

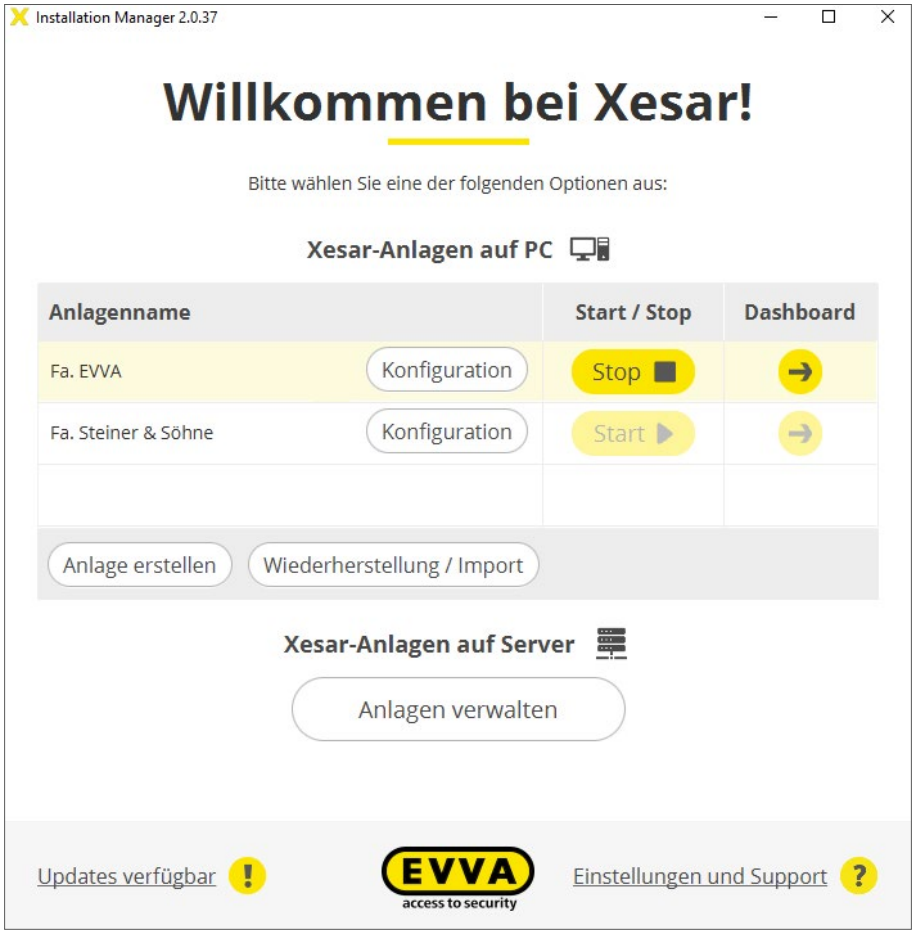


Nach erfolgreichem Update wird die aktuelle Versionsnummer auf der Konfigurationsseite der Anlage angezeigt.

15.6 Mehrere Anlagen auf einem PC verwalten

Im Installation-Manager können mehrere Anlagen verwaltet werden.

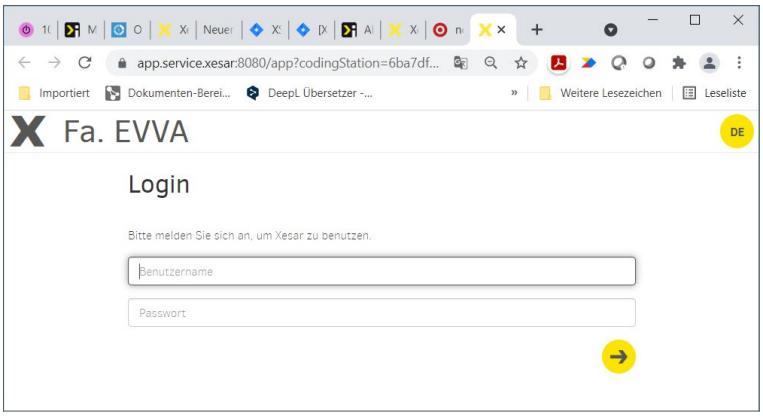
Es kann nur eine Anlage gestartet sein.



» Zur Erstellung einer weiteren Anlage klicken Sie auf den Button **Anlage erstellen** und folgen Sie der Anleitung.

15.7 Verwaltung einer gestarteten Anlage

» Klicken Sie auf den Button **Dashboard** , gelangen Sie zum Anlagen-Login im Browser.



» Melden Sie sich mit dem Benutzernamen **admin** als Anlagenadministrator mit dem entsprechenden Passwort vom Anlagensicherheitsblatt an.

Nach der Anmeldung als admin können Sie in der Kachel „Benutzer" das Passwort ändern und weitere Benutzer anlegen.

Der Systemadministrator (su) kann nur Benutzerpasswörter ändern.

16 Xesar-Anlagen auf Server

16.1 Installationsvoraussetzungen

Vor Start der Installation von Xesar-Anlagen müssen auf dem Anlagen-PC (Windows 10 Pro) Docker und der Treiber für die Codierstation installiert werden (siehe Kapitel „Docker-Installation").

16.2 Programme zur Installation und Verwaltung

Für die Erstellung und Verwaltung von Xesar-Anlagen auf Server benötigen Sie folgende Programme:

16.2.1 Installation-Manager

Mit dem Installation-Manager verwalten Sie eine oder mehrere Anlagen. Weiters werden Xesar-Systemeinstellungen vorgenommen.

Folgende Aufgaben können durchgeführt werden:

- Einfache Erstellung von Xesar-Anlagen auf PC bzw. Server
- Starten und Stoppen einer Anlage
- Verwaltung der Admin-Karte
- Durchführung von Updates
- Verwaltung von mehreren Anlagen.
- Aufladen von KeyCredits und KeyCredits Xesar-Lifetime
- Einstellen von automatischen Backups der gestarteten Anlage
- Tausch von defekten Admin-Karten
- Einstellen von Anlagen-Ports

16.2.2 Periphery-Manager

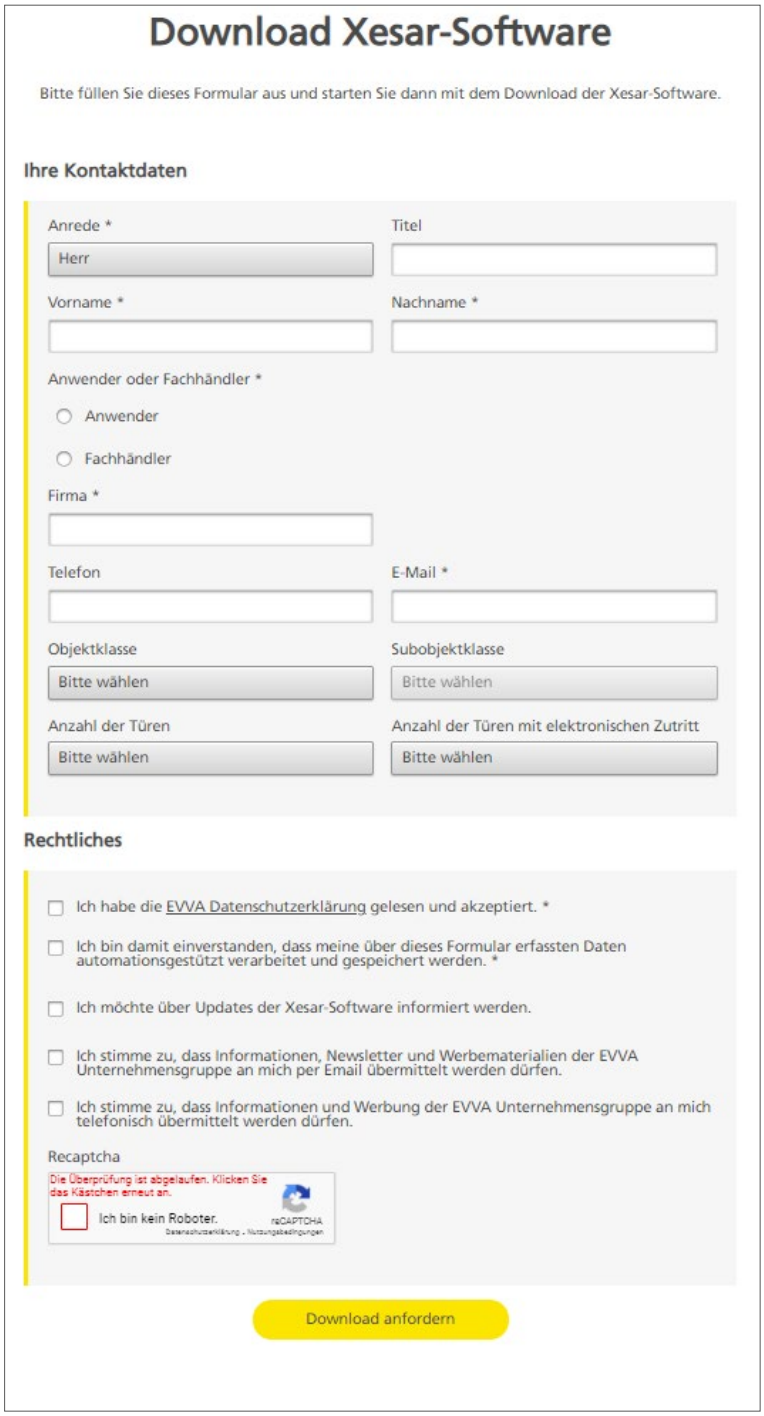
Der Periphery-Manager ermöglicht den Betrieb einer Codierstation an einem Administrator-PC und an Client-PCs bei einer Xesar-Anlage auf Server (Mehrplatz-Anlage).

Der Periphery-Manager kann in der **Xesar-Software > Support > Updates** heruntergeladen werden.

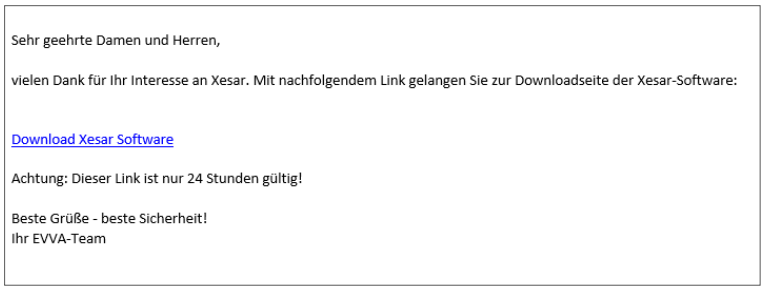
16.2.3 Xesar-Software

Die Xesar-Software ist eine Applikation, die aus dem Installation-Manager aufgerufen wird und in einem Browser läuft. Mit der Xesar-Software kann eine im Installation-Manager gestartete Anlage am Dashboard verwaltet werden.

Den Download des aktuellen Installation-Managers finden Sie auf der EVVA-Webseite im Tab Software.



» Füllen Sie das Formular „Download Xesar-Software" aus und senden Sie es ab.



Sehr geehrte Damen und Herren,

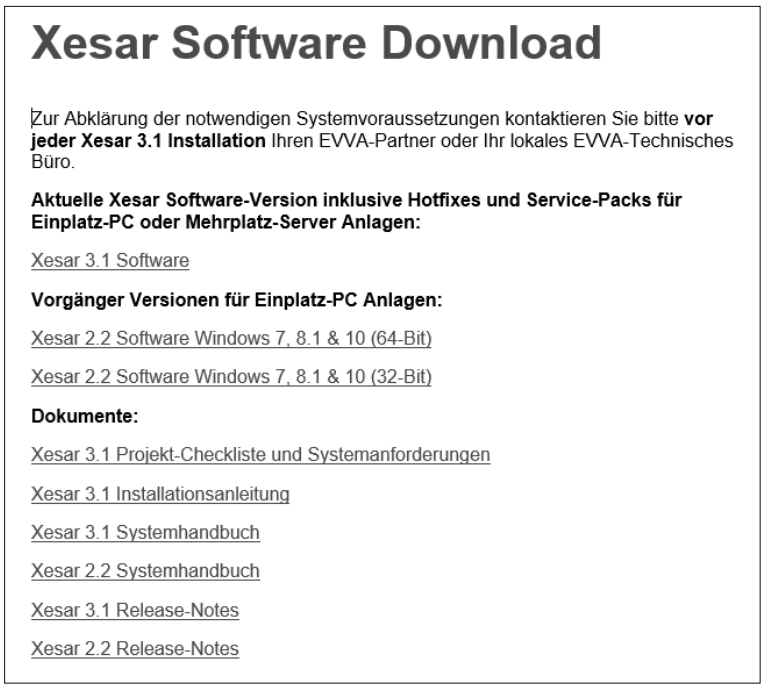
vielen Dank für Ihr Interesse an Xesar. Mit nachfolgendem Link gelangen Sie zur Downloadseite der Xesar-Software:

Download Xesar Software

Achtung: Dieser Link ist nur 24 Stunden gültig!

Beste Grüße - beste Sicherheit!
Ihr EVVA-Team

Sie erhalten an die im Formular „Download Xesar-Software" angegebene E-Mail-Adresse eine E-Mail mit einem zeitlich beschränkten Download-Link.



Xesar Software Download

Zur Abklärung der notwendigen Systemvoraussetzungen kontaktieren Sie bitte **vor jeder Xesar 3.1 Installation** Ihren EVVA-Partner oder Ihr lokales EVVA-Technisches Büro.

Aktuelle Xesar Software-Version inklusive Hotfixes und Service-Packs für Einplatz-PC oder Mehrplatz-Server Anlagen:

Xesar 3.1 Software

Vorgänger Versionen für Einplatz-PC Anlagen:

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

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

Dokumente:

Xesar 3.1 Projekt-Checkliste und Systemanforderungen

Xesar 3.1 Installationsanleitung

Xesar 3.1 Systemhandbuch

Xesar 2.2 Systemhandbuch

Xesar 3.1 Release-Notes

Xesar 2.2 Release-Notes

- Laden Sie die aktuelle Xesar-Software auf Ihren PC.
- Öffnen Sie mit Doppelklick die *.msi Datei.

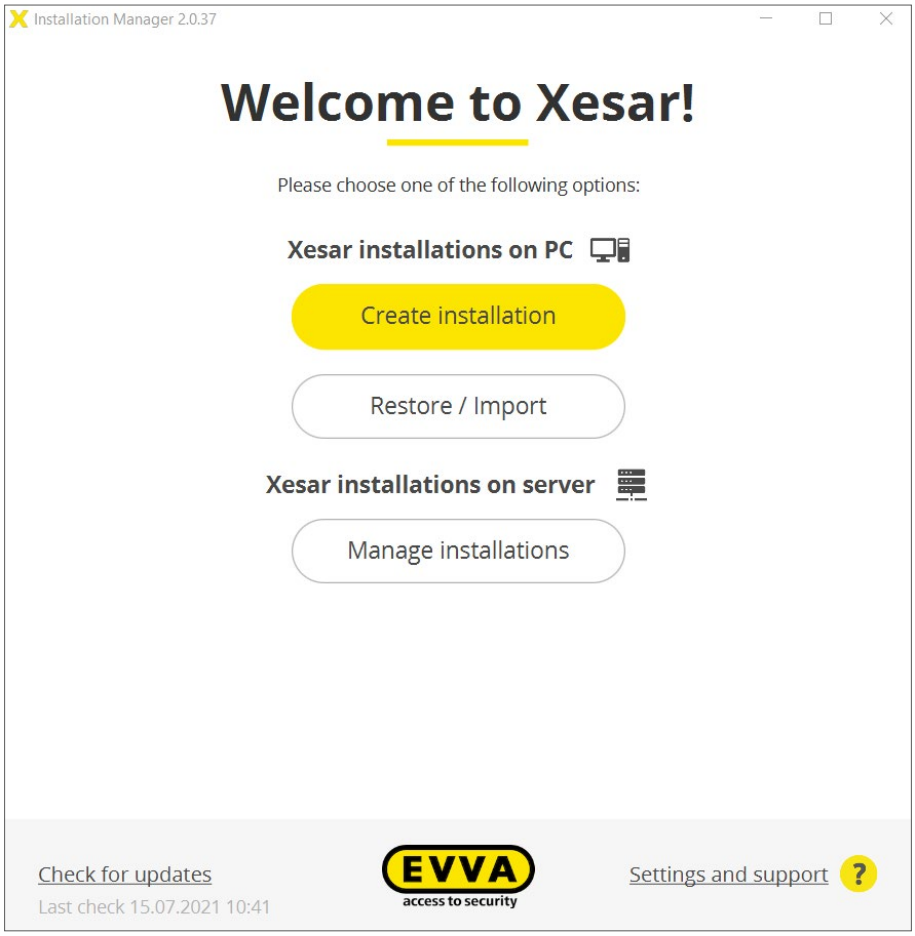
Der Installation-Manager wird installiert und eine Desktop- und eine Startmenüverknüpfung werden erstellt.

- Starten Sie den Installation-Manager mit Klick auf eine der Verknüpfungen.

16.3 Installationsablauf

» Starten Sie die EXE-Datei des Installation-Managers.

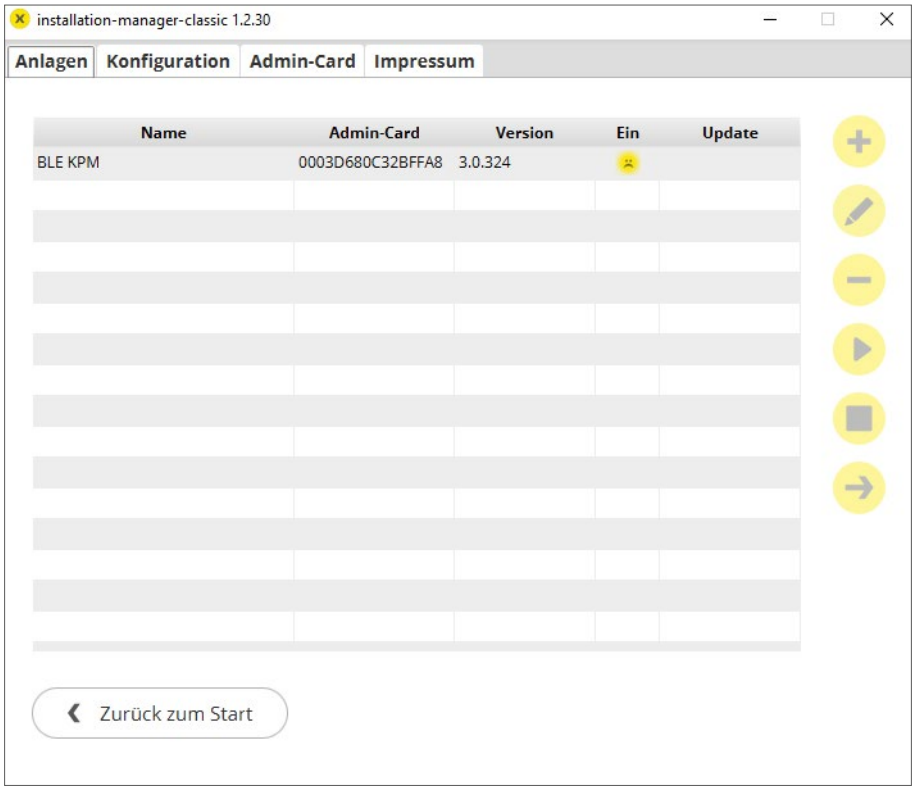
Fenster „Willkommen bei Xesar!" mit Installationswahl für Xesar-Anlagen auf PC bzw. Server:



16.3.1 Installation Xesar-Anlage auf Server

» Klicken Sie auf den Button **Server-Anlagen verwalten**, gelangen Sie zur Verwaltungsansicht von Anlagen auf Server.

Bei einem Update auf den neuen Installation-Manager werden bestehende Xesar-Anlagen auf Server automatisch in die Verwaltungsansicht der Xesar-Anlagen auf Server importiert.



Die Verwaltung von Xesar-Anlagen auf Server erfolgt laut nachfolgender Anleitung.

16.4 Starten und Beenden von Xesar-Anlagen auf Server

» Klicken Sie auf den von Ihrem Administrator bereitgestellten Link (Server)
oder
» Klicken Sie im Installation-Manager oder Periphery-Manager auf das Symbol **Gehe zu** .

Bevor Sie den Client-PC herunterfahren, beenden Sie den Periphery-Manager (wichtig für die Codierstation).

» Klicken Sie auf das Symbol **Stop** , um die Verbindung zwischen Periphery-Manager und Browser zu trennen.

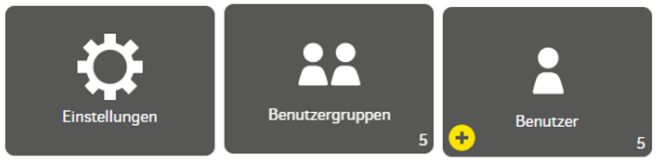
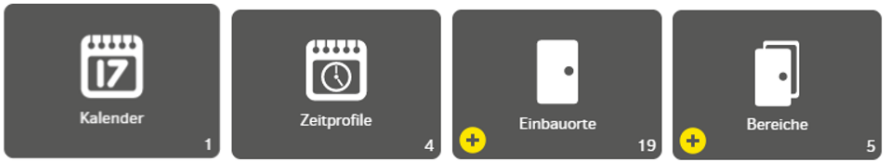
» Klicken Sie mit einem Rechtsklick auf das Symbol **Beenden** , um den Periphery-Manager zu beenden.

Das Symbol des Periphery Managers ist in der Taskleiste.

Der Periphery-Manager wird nicht beendet, wenn Sie auf das Symbol **x** im Programmfenster klicken.

Wenn Sie den Periphery-Manager nicht korrekt beenden, kann es zu einem Fehler beim nächsten Start des Periphery-Managers kommen. Der Periphery-Manager muss in diesem Fall neu eingerichtet werden.

17 Inbetriebnahme Xesar-Software

1. Schritt	
2. Schritt	
3. Schritt	
4. Schritt	

17.1 Allgemeines zur Inbetriebnahme

Neue Einstellungen und Änderungen müssen vor dem Verlassen der jeweiligen Seite gespeichert werden. Geschieht das nicht, bleiben die ursprünglichen Einstellungen erhalten.

Klicken Sie auf das Symbol **csv** oder **xlsx**. Alle Listen können als .csv- oder .xlsx-Datei exportiert und gedruckt werden. Als Dateiursprung muss dabei 65001: Unicode (UTF- 8) verwendet werden.

Pflichtfelder sind mit * gekennzeichnet.

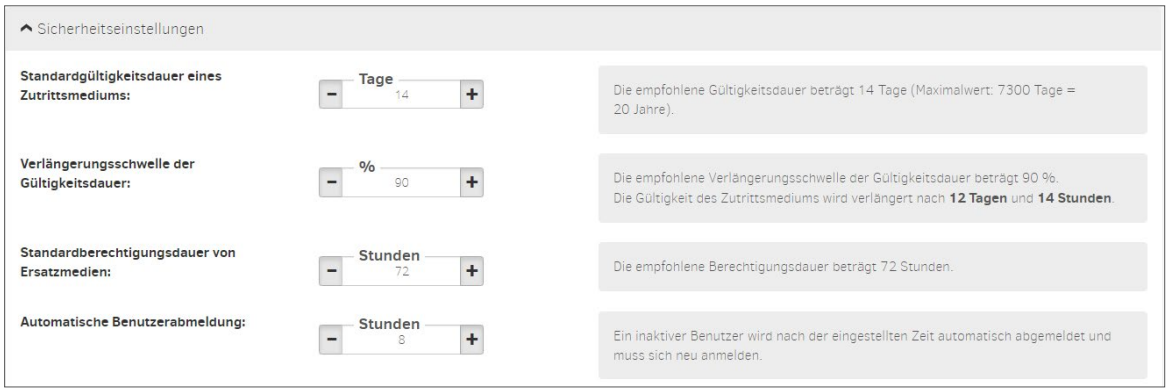
Klicken Sie auf das Symbol **?**, wird der entsprechende Hilfetext eingeblendet.

Mit einem Doppelklick auf die Spaltentrennlinie wird die Spaltenbreite an der Spaltenüberschrift angepasst.

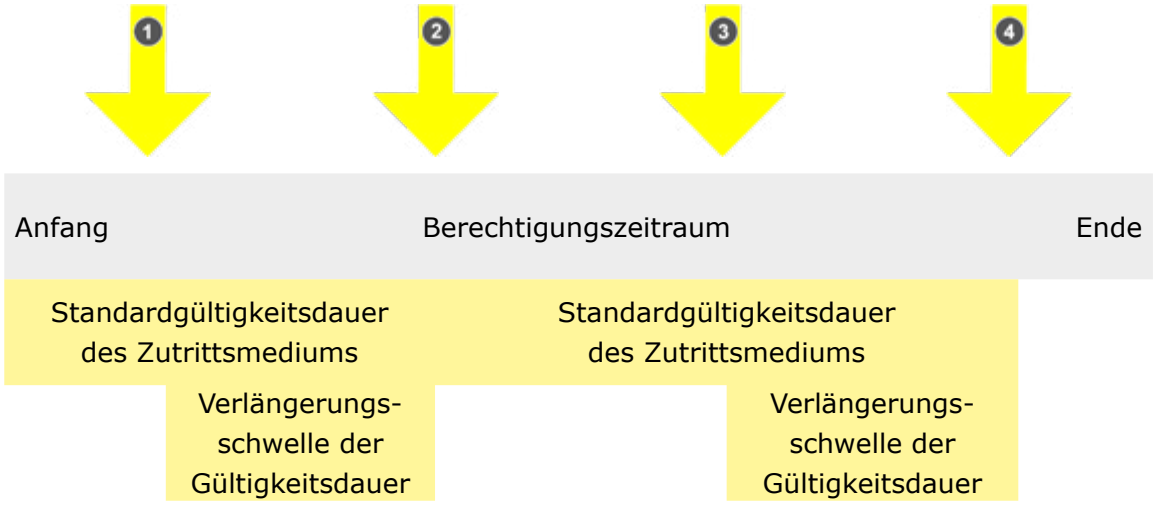
Das Ergebnis der aufbereiteten Liste ist abhängig von der Anzahl der Spalten und der Bildschirmdarstellung.

17.2 Einstellungen

17.2.1 Sicherheitseinstellungen



17.2.2 Gültigkeits- und Berechtigungsdauer der Zutrittsmedien



❶ Frühestmögliches Update
❷ Spätestmögliches Update
❸ Frühestmögliches Update
❹ Spätestmögliches Update

Standardgültigkeitsdauer des Zutrittsmediums:

Die Standardgültigkeitsdauer ist die voreingestellte Zeitdauer, in der das Zutrittsmedium nach Aktualisierung an der Codierstation oder am Xesar-Online-Wandleser gültig ist.

Die Standardgültigkeitsdauer kann bei Ausgabe von Zutrittsmedien individuell eingestellt werden.
Wenn die Standardgültigkeitsdauer abgelaufen ist, wird das Zutrittsmedium ungültig und muss gegebenenfalls an der Codierstation oder am Xesar-Online-Wandleser aktualisiert werden.
Je kürzer die Standardgültigkeitsdauer ist, desto sicherer ist die Anlage, da das Zutrittsmedium früher ungültig wird.

Die empfohlene Gültigkeitsdauer beträgt 14 Tage.

Die maximal einstellbare Gültigkeitsdauer beträgt 7300 Tage (ca. 20 Jahre).

Verlängerungsschwelle der Gültigkeitsdauer:

Die Verlängerungsschwelle der Gültigkeitsdauer definiert den Zeitbereich, in dem die Gültigkeitsdauer des Zutrittsmediums an der Codierstation oder am Xesar-Online-Wandleser verlängert wird.

Standardberechtigungsdauer von Ersatzmedien:

Die Standardberechtigungsdauer von Ersatzmedien beträgt laut Systemvoreinstellung 72 Stunden. Die Standardberechtigungsdauer kann bei der Ausgabe von Ersatzmedien individuell eingestellt werden (siehe Kapitel „Zutrittsmedien“).

Automatische Benutzerabmeldung:

Nach der eingestellten Zeit in Stunden wird der Benutzer (z. B. Empfang, Administrator oder Wartungstechniker) aus Sicherheitsgründen automatisch von der Benutzeranmeldung (Benutzer und Login) abgemeldet. Zur Bedienung der Xesar-Software muss sich der entsprechende Benutzer wieder anmelden.

17.2.3 Systemeinstellungen

IP-Adresse des Servers:

Die IP-Adresse wird für die Verbindung der Codierstation mit dem Server benötigt (die IP-Adresse wird in die Konfigurationsdatei geschrieben). Zusätzlich wird die IP-Adresse beim Hinzufügen einer Codierstation zur Anlage benötigt.

Bei der lokalen Installation wird im Eingabefeld automatisch die IP-Adresse der lokalen Installation angezeigt.

Tägliche Ausführungszeit:

Die tägliche Ausführungszeit ist der Zeitpunkt der Systemzeit-Synchronisation. Zusätzlich wird die tägliche Ausführungszeit für folgende Konfigurationseinstellungen des Xesar-Online-Wandlesers mit der Xesar-Software (Backend) verwendet.

- Vollständige Blacklist-Übertragung an die Online-Wandleser. Sicher gesperrte Zutrittsmedien werden von der Blacklist entfernt.
- Personenbezogene Ereigniseinträge werden nach Ablauf der definierten Zeit anonymisiert.
- Drei Monate vor der ersten Zeitumstellung im Jahr werden Wartungsaufgaben generiert.
- Erstellung von Wartungsaufgaben zum Aktualisieren der Kalendertage auf den Komponenten.
- Der Backup-Status wird aktualisiert.

Wählen Sie als tägliche Ausführungszeit immer einen Zeitpunkt, zu dem die Anlage läuft und der Xesar-Online-Wandleser online ist (z. B. Office-Zeiten)!

Logo:

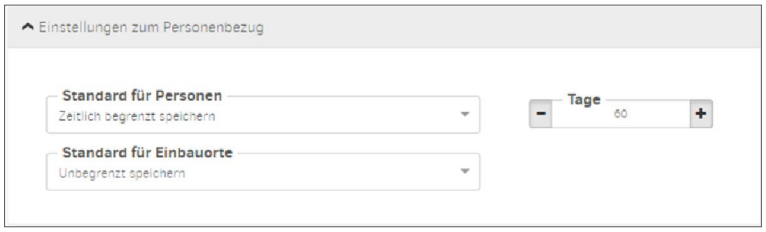
Das Logo wird am Dashboard vor dem Installationsnamen angezeigt. Wenn Sie ein individuelles Logo hinzufügen möchten, sind folgende Spezifikationen zu beachten:

Maximale Dateigrößes: 2 MB
Mögliche Dateitypen: jpg, png, gif, svg

Einstellungen zum Personenbezug:

Die Einstellungen zum Personenbezug geben an, ob und wie lange personenbezogene Ereignisdaten gespeichert werden.

Beachten Sie bei den Einstellungen die datenschutzrechtlichen Anforderungen Ihres Unternehmens.



Es gibt 3 Datenspeichereinstellungen für Personen und Einbauorte:

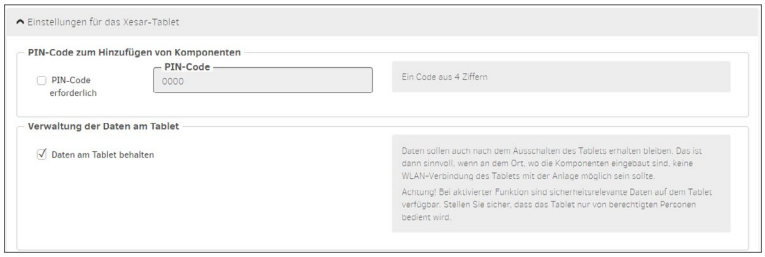
- Nicht speichern
- Unbegrenzt speichern
- Zeitlich begrenzt speichern (Einstellbereich in Tagen)

Personen- und komponentenspezifische Einstellungen werden bei den Kacheln „Personen" oder „Einbauorte – Komponente" festgelegt.

Einstellungen für das Xesar-Tablet:
Aus sicherheitstechnischen Gründen ist die Benutzung des Xesar-Tablets für anlagenrelevante Wartungsaufgaben mit einem PIN-Code geschützt. Die PIN-Code Abfrage am Tablet kann deaktiviert werden.

Verwaltung der Daten am Xesar-Tablet:
Das Behalten der Daten am Tablet nach Abschalten des Tablets kann aktiviert werden.

Ändern Sie den voreingestellten PIN-Code bei der Erstinbetriebnahme des Xesar-Tablets.



17.3 Benutzergruppen

In den Benutzergruppen werden die Berechtigungen für Benutzer definiert.

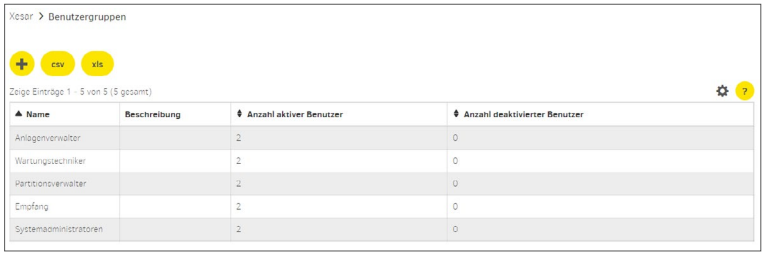
Benutzer verwalten die Anlage über die Xesar-Software. Es können beliebig viele Benutzer mit unterschiedlichen Berechtigungen (abhängig von der Funktion) angelegt werden. Diese unterschiedlichen Berechtigungen werden in den Benutzergruppen definiert.

Ansicht aller vordefinierten Benutzergruppen:

Die vordefinierten Benutzergruppen können Benutzern zugewiesen werden. Vordefinierte Benutzergruppen können nicht gelöscht werden.

Einem Benutzer können mehrere Benutzergruppen zugewiesen werden.

Beachten Sie: Bei der Vergabe mehrerer Benutzergruppen addieren sich die Berechtigungen für den entsprechenden Benutzer.



Folgende vordefinierte Benutzergruppen stehen zur Auswahl:

Systemadministrator
darf nur die Benutzerpasswörter ändern

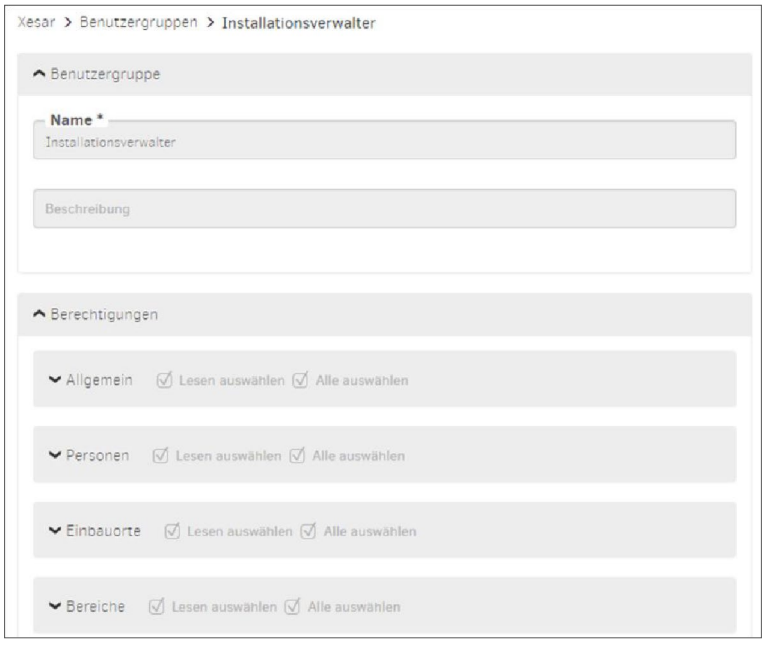
Installationsverwalter
hat alle Berechtigungen, ausgenommen Benutzerpasswörter zu ändern

Wartungstechniker
hat eingeschränkte, wartungsrelevante Berechtigungen

Partitionsverwalter
hat eingeschränkte, verwaltungsrelevante Berechtigungen

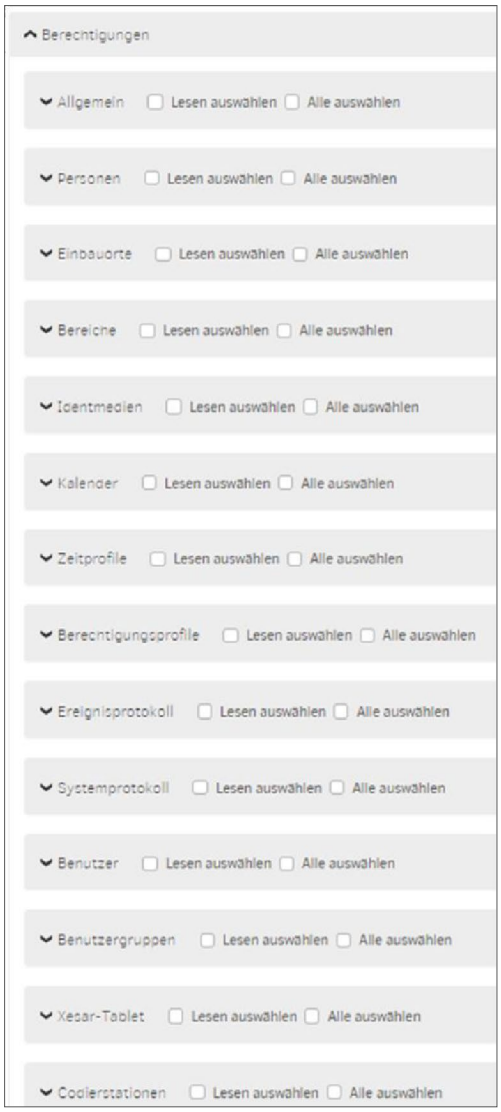
Empfang
hat eingeschränkte, empfangsrelevante Berechtigungen

Beispiel Benutzergruppe Installationsverwalter
Die Benutzer in der Benutzergruppe haben alle Lese- und Bearbeitungsberechtigungen:



Die Berechtigungen der vordefinierten Benutzergruppen können nicht verändert werden.

Kopieren Sie bei Bedarf eine vordefinierte Benutzergruppe und verändern Sie die Berechtigungen. Speichern Sie diese individuelle Benutzergruppe mit einem sprechenden Namen ab.

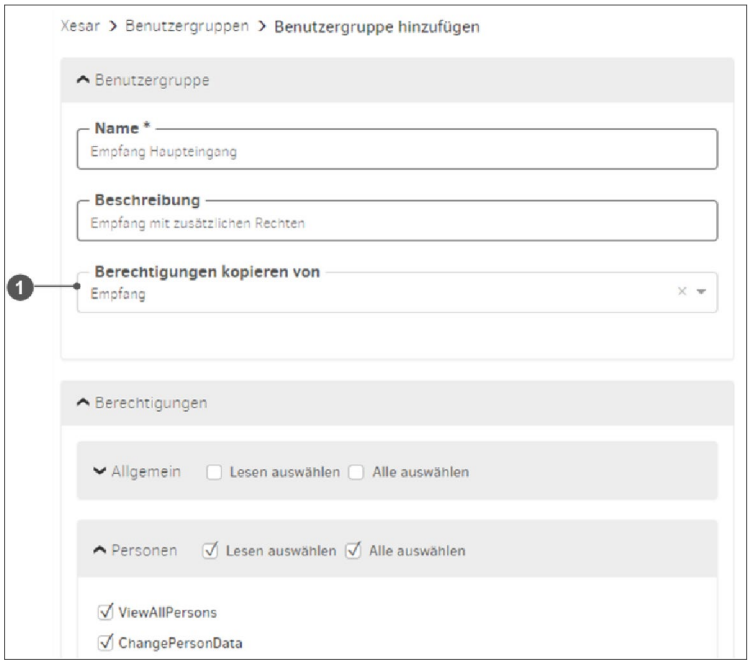


Die Berechtigungen sind nach den Kacheln am Dashboard gruppiert.

In jeder Berechtigungsgruppe werden folgende Berechtigungen definiert:

- nur Leseberechtigungen
- alle Berechtigungen ausgewählt werden.

Beispiel Individuelle Benutzergruppe – Empfang Haupteingang mit Basis Benutzergruppe Empfang ❶ und zusätzlichen Lese- und Bearbeitungsrechten für Personeneinstellungen:



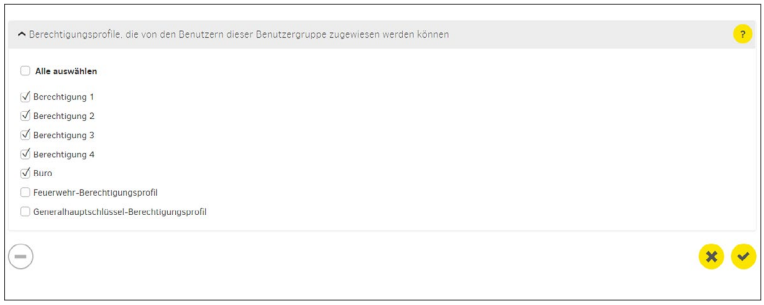
Verwenden Sie zur Vergabe von Berechtigungen für Benutzer als Basis die vordefinierten Benutzergruppen.

Bei Bedarf können spezielle Berechtigungsgruppen generiert werden. Kontaktieren Sie in diesem Fall das technische Büro von EVVA.

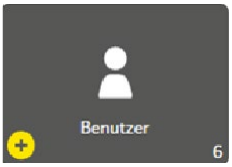
Zuweisungsmöglichkeit des Berechtigungsprofils einschränken:

Nur ausgewählte Berechtigungsprofile können von Benutzern der entsprechenden Benutzergruppen zugewiesen werden.

Beispiel:
Benutzer der Benutzergruppe Empfang dürfen z. B. nur die Berechtigungsprofile Mitarbeiter, Praktikant, Reinigung und Schichtarbeiter Zutrittsmedien zuweisen. Die Benutzer der anderen Benutzergruppen dürfen zusätzlich die Berechtigungsprofile Chef und Assistentin, Feuerwehr- sowie Master Key-Berechtigungsprofil einem Zutrittsmedium zuweisen.



17.4 Benutzer



Benutzer verwalten die Anlage über die Xesar-Software. Es können beliebig viele Benutzer mit unterschiedlichen Berechtigungen (abhängig von der Funktion) angelegt werden.

Mit dem Symbol „**Hinzufügen**" kann ein neuer Benutzer hinzugefügt werden. Die Anzahl der angelegten Benutzer wird in der Kachel „Benutzer" angezeigt.

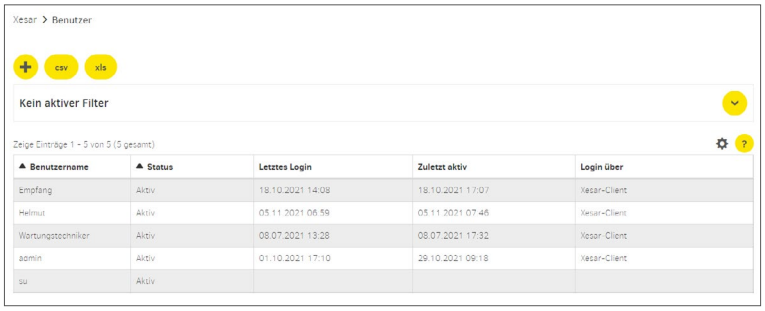
Benutzer sind auch Personen, die in der Anlage mit Ihnen zugewiesenen Zutrittsmedien Zutrittsberechtigungen haben.

In der Benutzer-Übersichtsliste werden alle angelegten Benutzer angezeigt.

Die bereits in der Erstinstallation vordefinierten Benutzer **su** (Superadministrator) und **admin** (Administrator) können nicht verändert oder gelöscht werden.

- **su**
  hat nur die Berechtigung als Systemadministrator Benutzerpasswörter zu ändern

- **admin**
  hat alle Berechtigungen



Neuer Benutzer:

Wenn Sie einen neuen Benutzer anlegen möchten, stehen folgende Eingabefelder zur Auswahl:

Pflichtfelder sind mit * gekennzeichnet.

Benutzername
des neuen Benutzers, z. B. Verwalter 1

Beschreibung
mit ergänzenden Informationen zum neuen Benutzers

Passwort
für die Anmeldung (Login).
Mindestens 6 Zeichen; zusätzlich wird eine Bewertung des Sicherheitsgrades des Passwortes angezeigt.

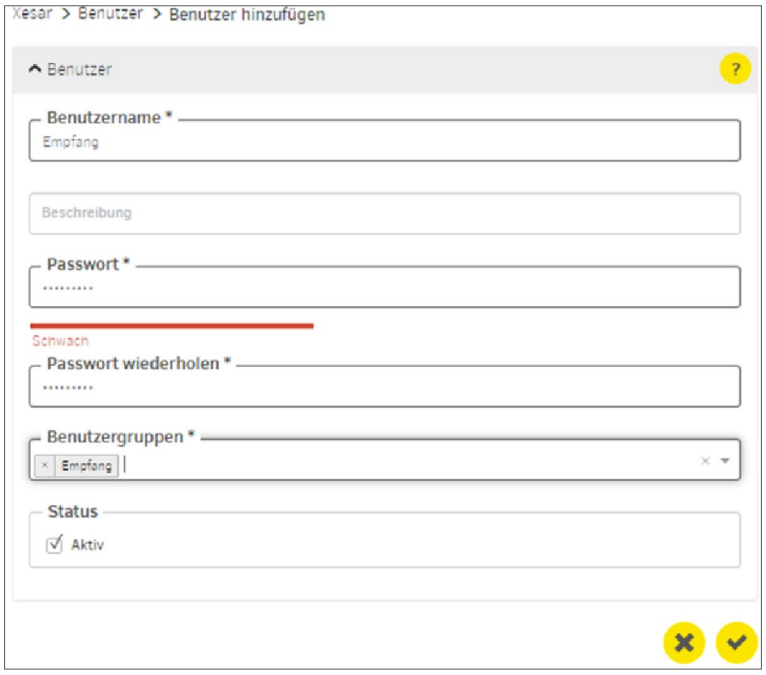
Passwort wiederholen
Das gewählte Passwort nochmals eingeben.

Benutzergruppen
Auswahl der definierten Benutzergruppen für den Benutzer. Es muss mindestens eine Benutzergruppe ausgewählt werden.

Person
(Dieses Feld wird erst nach dem ersten Speichern angezeigt)

Die Funktion des Benutzers kann einer Person zugewiesen werden,
z. B. Wartungstechniker1 > Hans Huber.
Der Personenbezug hat reinen Informationswert und keine funktionellen Auswirkungen.

Status
Benutzer können vom admin auf aktiv oder inaktiv gesetzt werden. Inaktive Benutzer können sich nicht anmelden.



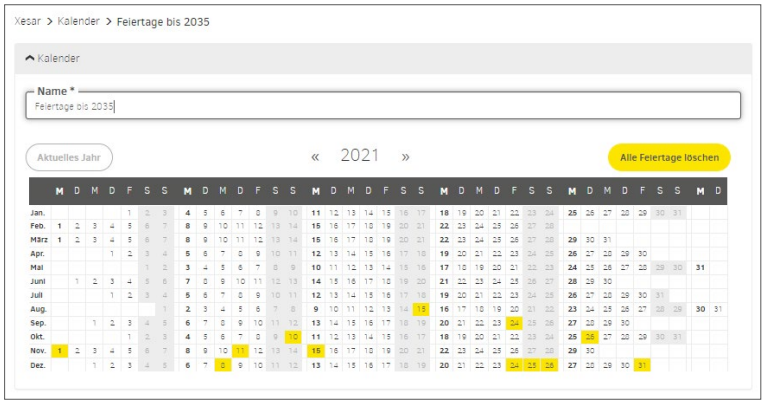
Konfiguration herunterladen
Das jeweilige Benutzerzertifikat (Konfiguration) wird heruntergeladen. Das Benutzerzertifikat wird für eine gesicherte Drittsystemschnittstellen-Aktionen (z. B. Personen-Datenimport über die Drittsystemschnittstelle) benötigt.

17.5 Kalender

Mit der Kalenderfunktion verwalten Sie Sondertage, wie z. B. Feiertage oder Betriebsurlaube für ein Kalenderjahr. An diesen Sondertagen sind Ausnahmen von den Zeitprofilen möglich. Die Anzahl der Kalender wird in der Kachel „Kalender" angezeigt.

Es können maximal 5 Kalender mit in Summe 50 unterschiedlichen Sondertagen definiert werden.

Ein Sondertag (z.B. Weihnachten) darf nur in einem Kalender vorkommen.



Kalender importieren

Sie können bestehende Kalender mit dem Dateiformat .ics oder .csv importieren und weiterverarbeiten.

Es können keine Kalender importiert werden, in denen der aktuelle Tag als Sondertag gekennzeichnet ist.

17.6 Zeitprofile

In Zeitprofilen werden sowohl Office-Mode-Zeitprofile (automatische Daueröffnung für Xesar-Zutrittskomponenten) als auch Zeitprofile für Berechtigungsprofile von Personen bzw. Zutrittsmedien definiert.

Zusätzlich werden Schließzeitpunkte zur automatischen Beendigung eines manuellen Office-Mode (manuelle Daueröffnung) festgelegt.

Wird einer Xesar-Zutrittskomponente kein Office-Mode-Zeitprofil zugewiesen, haben nur berechtigte Zutrittsmedien Zutritt.

Wird bei der Erstellung eines Zutrittsmediums kein Zeitprofil verwendet, gilt für dieses Zutrittsmedium keine Zutrittszeiteinschränkung – das Zutrittsmedium hat also Dauerzutritt.

Office-Mode:

Unter Office-Mode wird in Xesar die automatische und zeitgesteuerte Dauerfreigabe von Xesar-Zutrittskomponenten verstanden. Die Xesar-Komponenten mit Office-Mode ermöglichen im definierten Zeitfenster den Zutritt auch ohne Zutrittsmedium.

Beispiel:
Ein Geschäftslokal hat Öffnungszeiten von 08:00 bis 16:00 Uhr. Das Office-Mode-Zeitprofil ist von 08:00 bis 16:00 Uhr.

Der Zutritt durch die Eingangstür zum Geschäftslokal mit diesem Zeitprofil kann zwischen 8:00 und 16:00 Uhr für alle Personen ohne Zutrittsmedium erfolgen. Die Xesar-Zutrittskomponente schaltet automatisch um 08:00 Uhr auf **Öffnen** und um 16:00 Uhr auf **Schließen**.

Der Office-Mode kann jederzeit manuell mit einem berechtigten Zutrittsmedium beendet werden.

Shop-Mode:

Der Shop-Mode ist eine Erweiterung zum Office-Mode. Dabei wird der Office-Mode nicht automatisch zum definierten Zeitpunkt gestartet, sondern erst nach einmaliger Identifizierung mit einem berechtigten Zutrittsmedium.

Beispiel:
Für ein Geschäft wurde ein Office-Mode mit dem Zeitfenster von 08:00 bis 16:00 Uhr festgelegt.
Zusätzlich ist an der Xesar-Zutrittskomponente der Eingangstür der Shop-Mode aktiviert.
Wenn sich nun ein Mitarbeiter mit berechtigtem Zutrittsmedium verspätet und nicht vor oder um 08:00 Uhr im Geschäft ist, bleibt die Eingangstür trotz Office-Mode geschlossen. Erst wenn der Mitarbeiter (auch nach 08:00 Uhr) ins Geschäft kommt und mit dem berechtigten Zutrittsmedium öffnet, wird der Office-Mode gestartet.

Mit dieser Einschränkung wird verhindert, dass der Office-Mode automatisch öffnet, auch wenn kein Mitarbeiter im Geschäft ist.

Manual Office-Mode:

Unter Manual Office-Mode wird in Xesar die manuelle Aktivierung einer Dauerfreigabe von Xesar-Zutrittskomponenten verstanden. Für die Funktion muss sowohl die entsprechende Xesar-Zutrittskomponente als auch das entsprechende Zutrittsmedium über das Berechtigungsprofil berechtigt sein. Den Manual Office-Mode stellen Sie im jeweiligen Menüpunkt unter **Einbauorte** und **Berechtigungsprofile** ein.

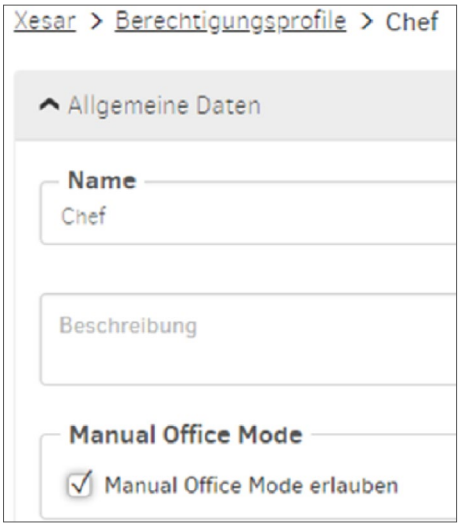
Der Manual Office-Mode wird durch zweimaliges Anhalten eines berechtigten Zutrittsmediums an der Xesar-Zutrittskomponente aktiviert. Sie erhalten eine entsprechende optische und akustische Bestätigung (siehe Kapitel „Ereignissignalisierung“).

Der Manual Office-Mode wird automatisch zum definierten Schließzeitpunkt beendet oder manuell, durch erneutes, zweimaliges Anhalten eines berechtigten Zutrittsmediums an der Xesar-Zutrittskomponente. Sie erhalten eine entsprechende optische und akustische Bestätigung (siehe Kapitel „Ereignissignalisierung“).

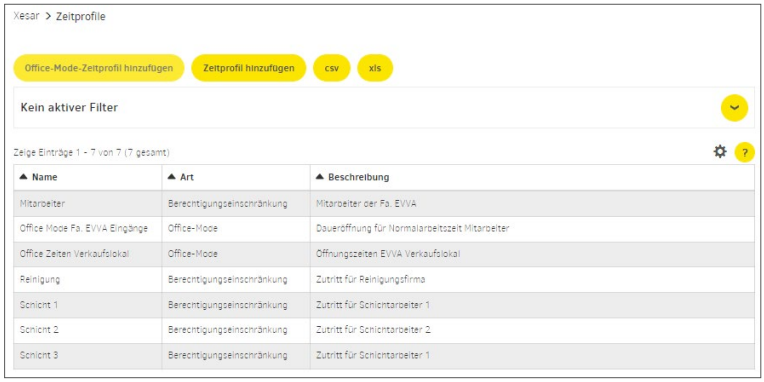
Manual Office-Mode und Shop-Mode aktivieren:

» Öffnen Sie **Xesar > Einbauorte > Haupteingang**

» Öffnen Sie X**esar > Berechtigungsprofile > Benutzer**



Ansicht Zeitprofile:



Die Eingabe der Zeiten in den Eingabefeldern kann numerisch oder mittels Pfeiltasten erfolgen.

17.6.1 Office-Mode Zeitprofil hinzufügen

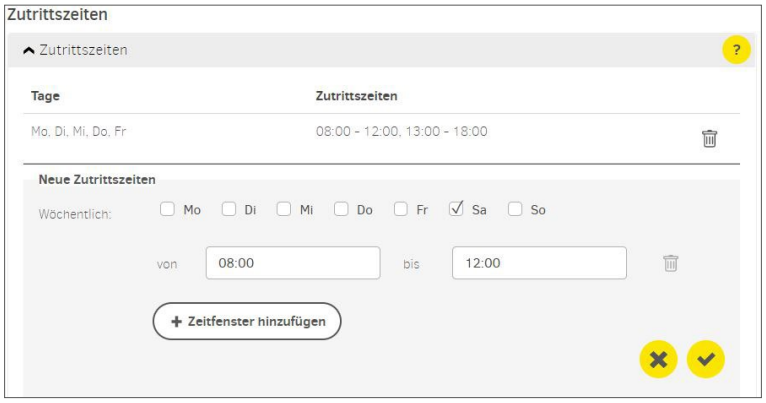
Die Funktion „Daueröffnung" gilt für Xesar-Zutrittskomponenten.

Zu definierten Zeiten ist der Zutritt ohne Berechtigung möglich. Die Xesar-Zutrittskomponente ist also zum Öffnen der Tür bereit.

Es können maximal 24 Zeitserien definiert werden.

Es können in Summe maximal 5 unterschiedliche Zeitfenster oder Zeitpunkte pro Wochentag oder Kalender hinzugefügt werden.

Beispiel Office-Zeiten Parteienverkehr:
Montag bis Freitag von 8:00 bis 12:00 Uhr sowie 13:00 bis 18:00 Uhr und Samstag von 8:00 bis 12:00 Uhr.



Zutrittszeiten an Feiertagen definieren Abweichungen von Zeitserien, an denen geänderte Zutrittszeiten oder Zutrittsverbote gelten.

„Keine Zutrittszeiten" bedeutet, dass an definierten Feiertagen im Kalender kein Zutritt möglich ist. Alle vorhandenen Kalender werden angezeigt.

Automatische Schließzeitpunkte:

Automatische Schließzeitpunkte definieren Zeitpunkte, zu denen der manuelle Office-Mode (manuelle Dauerfreigabe) automatisch endet. Damit wird gewährleistet, dass ein manuell gestarteter Office-Mode zum definierten Zeitpunkt sicher beendet wird.

Der manuelle Office-Mode kann nur an dafür definierten Xesar-Zutrittskomponenten und mit berechtigten Zutrittsmedien durch zweimaliges Anhalten an der Xesar-Zutrittskomponente aktiviert werden.

Es sind maximal 35 Zeitpunktserien möglich.

Beispiel:
Schließzeitpunkt Montag bis Freitag, jeweils 20:00 Uhr

Automatische Schließzeitpunkte an Feiertagen:

Für Sonder- oder Feiertage kann der Schließzeitpunkt geändert werden.

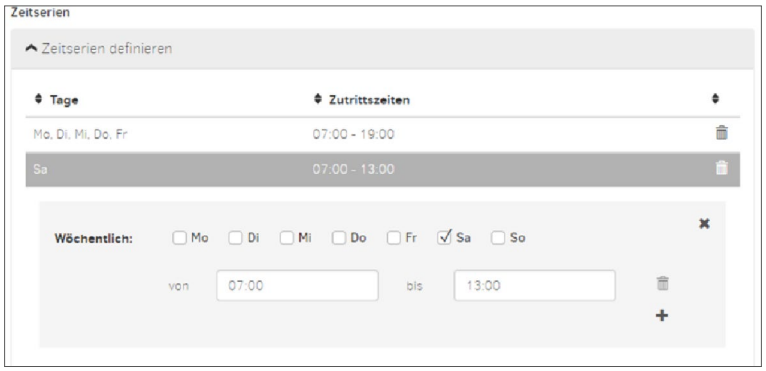
17.6.2 Zeitprofil hinzufügen

Zeitprofile können für Personen und Zutrittsmedien hinzugefügt werden.

Es können maximal 24 Zeitserien definiert werden.

Berechtigungseinschränkung:

Beispiel Zutrittszeiten für Mitarbeiter:
Montag bis Freitag von 7:00 bis 19:00 Uhr und
Samstag von 7:00 bis 13:00 Uhr.

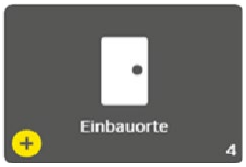


Zeitserienausnahmen:

Zeitserienausnahmen definieren Abweichungen von Zeitserien, wie z. B. Feiertage, an denen geänderte Zutrittszeiten oder Zutrittsverbote gelten.

Keine Zeitserie bedeutet, dass an definierten Feiertagen im Kalender kein Zutritt ist. Alle vorhandenen Kalender werden angezeigt.

17.7 Einbauorte



Alle Einbauorte mit Zutrittskomponenten einer Anlage werden im Bereich Einbauorte angelegt und definiert. Ein Einbauort kann eine Tür oder eine andere Anwendung, z. B. Lift sein.

Liste der Einbauorte:

Online Zustand:
beschreibt ob eine Komponente onlinefähig ist und ob sie mit der Xesar-Software verbunden ist

ID:
Eindeutige Identifikation (Bezeichnung), z. B. Raumnummer laut Gebäudeplan

Name:
Eindeutiger Name bzw. Bezeichnung, z. B. Haupteingang

Beschreibung:
Freie Beschreibung des Einbauortes zur besseren Erklärung z. B. Zentraler Zugang, Fluchtweg zu Sammelplatz

Art:
Frei definierbar, z. B. Glastür, Spind oder Automatiktür

Komponententyp:
verbaute Komponente am Einbauort

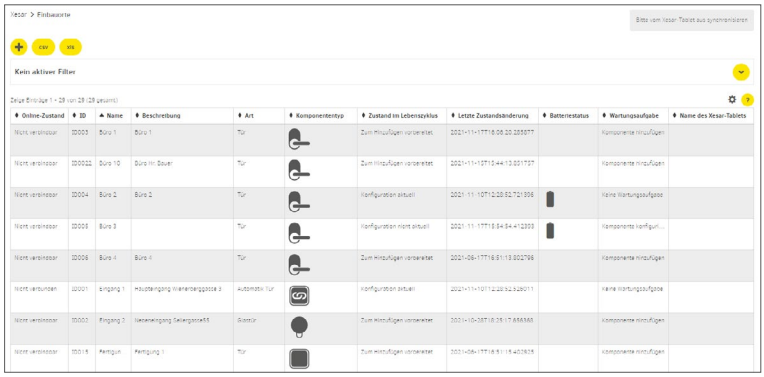
Zustand im Lebenszyklus:
beschreibt den aktuellen Zustand der Komponente z. B. zum Hinzufügen vorbereitet

Letzte Zustandsänderung:
Zeitpunkt der letzten Synchronisation der Komponente mit der Xesar-Software

Batteriezustand:
Anzeige des Batteriestatus der Komponente: Voll oder Leer

Wartungsaufgabe:
zeigt offene Wartungsaufgaben des Einbauortes an z. B. Komponente konfigurieren, entfernen, hinzufügen, FW-Update

Name des Xesar-Tablets:
Name des Tablets mit der synchronisierten offenen Wartungsaufgabe des Einbauorts



17.7.1 Einbauort hinzufügen

Wählen Sie die gewünschte Zutrittskomponente aus.

17.7.2 Einbauort beschreiben

Wenn Sie einen neuen Einbauort anlegen möchten, stehen folgende Eingabefelder zur Auswahl:

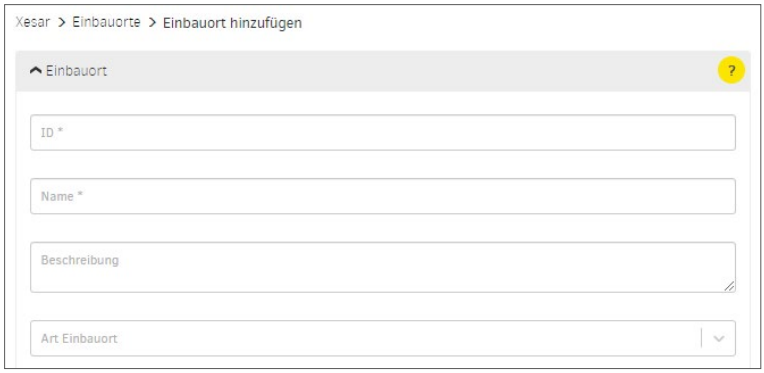
Pflichtfelder sind mit * gekennzeichnet.

ID:
Eindeutige Identifikation (Bezeichnung), z. B. Raumnummer laut Gebäudeplan

Name:
Eindeutiger Name bzw. Bezeichnung, z. B. Haupteingang

Beschreibung:
Freie Beschreibung des Einbauortes zur besseren Erklärung z. B. Zentraler Zugang, Fluchtweg zu Sammelplatz Wienerbergstraße

Art Einbauort:
Frei definierbar, z. B. Glastür, Spind oder Automatiktür



Öffnungsdauer:
Die Öffnungsdauer definiert die Zeit, die die Zutrittskomponente nach Berechtigung Zutritt gewährt, bevor sie wieder auskuppelt (sperrt). Die entsprechende Öffnungsdauer ist **Kurz** oder **Lang**. Die Öffnungsdauer wird bei der jeweiligen Person oder dem Zutrittsmedium definiert und bei Berechtigung an der Zutrittskomponente ausgelöst.

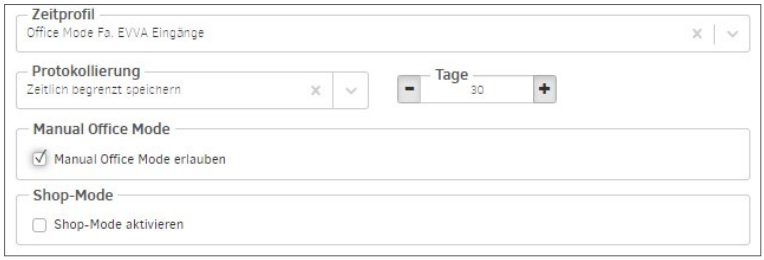
Die Zuordnung der Öffnungsdauer zur Person bzw. dem Zutrittsmedium erfolgt bei den Personen- und Zutrittsmedieneinstellungen.

Zeitprofil:
Auswahl des Office-Mode-Zeitprofils

Protokollierung:
Festlegung der Zutrittsereignis-Aufzeichnungsart und der Daten-Aufzeichnungsdauer

Manual Office-Mode:
Manueller Office Mode ist aktiv oder nicht aktiv

Shop-Mode:
Shop Mode ist aktiv oder nicht aktiv



Der **Office-Mode** ist die zeitgesteuerte Daueröffnung der Zutrittskomponente. Im definierten Zeitraum – z. B. Parteienverkehr oder Geschäftsöffnungszeiten – ist der Zutritt ohne Berechtigung möglich.

Der **Shop-Mode** wird erst mit Anhalten eines berechtigten Zutrittsmediums an der Zutrittskomponente gestartet.

17.8 Bereiche

Einbauorte können zu Bereichen zusammengeführt werden. Dies ist sinnvoll, wenn mehrere Einbauorte gleiche Eigenschaften, wie z. B. die gleichen Berechtigungen oder organisatorische Zusammengehörigkeit, wie Abteilungen oder Gebäudeabschnitte, haben.

Je Anlage (Partition) können maximal 95 Bereiche frei definiert werden.

Der Bereich Installation wird automatisch bei der Erstellung der Anlage erzeugt. Er beinhaltet alle Einbauorte und kann nicht geändert oder gelöscht werden.

Wenn dieser Bereich für ein Berechtigungsprofil ausgewählt wird, sind alle Einbauorte betroffen.

Der Import einer Xesar 2.2 Anlage mit 96 Bereichen ist nicht möglich. Entfernen Sie daher vor dem Import in der Xesar 2.2-Anlage einen Bereich.

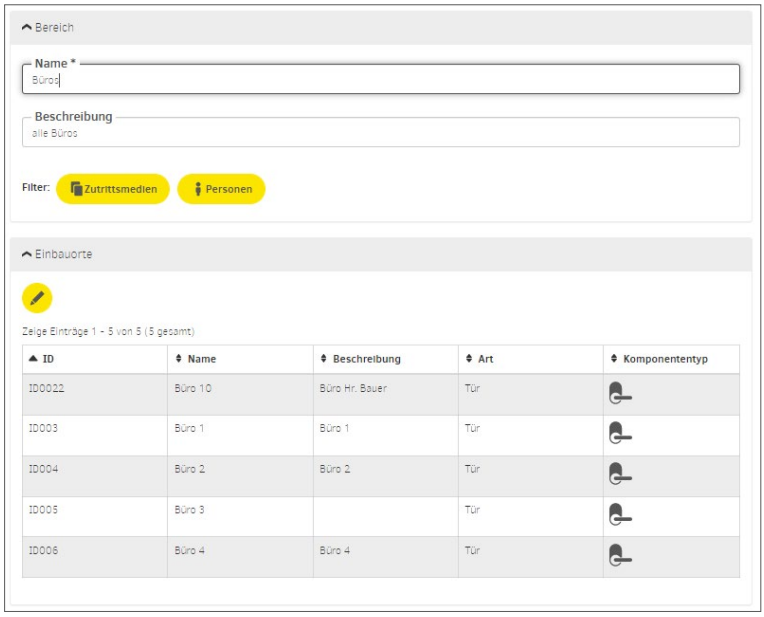
Name	Beschreibung	Anzahl Einbauorte
1. OG	alle Türen 1.OG	6
2. OG	alle Türen 2. OG	8
Aussentüren	alle EVVA Außentüren	3
Büros	alle Büros	3
EG	alle Türen EG	7
Fertigung	alle Fertigungstüren	3
Installation		29

Beispiel Anzeige Bereich Büros:
Pflichtfelder sind mit * gekennzeichnet.

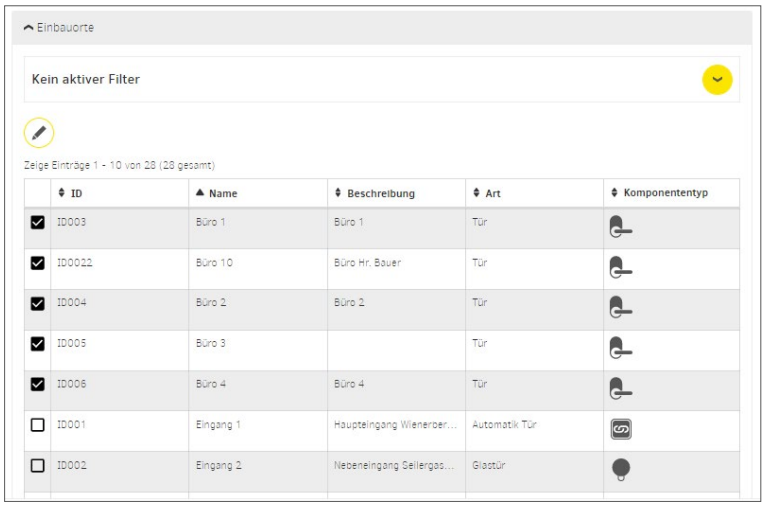
Name:
Name des Bereichs

Beschreibung:
Ergänzende Informationen zum Namen

Einbauorte:
Anzeige der ausgewählten Einbauorte



Auswahl von Einbauorten:
Wählen Sie die Einbauorte für den Bereich aus, indem Sie in der ersten Spalte das Feld aktivieren.



17.9 Berechtigungsprofile

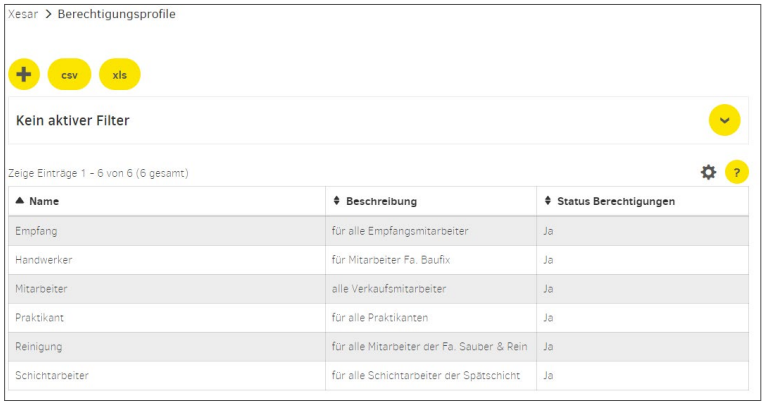
Berechtigungsprofile beschreiben räumliche und zeitliche Zutrittsbeschränkungen für Zutrittsmedien. Diese Zutrittsmedien können Personen zugewiesen werden. Das heißt, eine Person mit einem Zutrittsmedium hat nur zu den im Berechtigungsprofil definierten Einbauorten und Bereichen sowie nur zu den definierten Zeiten Zutritt. An anderen Orten und außerhalb der definierten Zeiten wird der Zutritt verweigert.

Ein Berechtigungsprofil kann vielen Zutrittsmedien zugewiesen werden (z. B. allen Personen einer Abteilung mit gleichen Berechtigungen).

Jedem Zutrittsmedium kann nur ein Berechtigungsprofil zugewiesen werden. Zusätzlich zu diesem Berechtigungsprofil können jedem Zutrittsmedium noch maximal 3 Individualberechtigungen für Einbauorte bzw. Bereiche mit Zeitprofilen zugewiesen werden. (Das ist z. B. notwendig für den Zutritt zu Spindschränken.)

Sind einem Berechtigungsprofil keine Einbauorte oder Bereiche zugewiesen, steht in der Übersichtsliste in der Spalte **Status Berechtigungen** der Eintrag **Nein**.

Es dürfen einem Berechtigungsprofil max. 32 Einbauorte zugewiesen werden.



Berechtigungsprofil:

Pflichtfelder sind mit * gekennzeichnet.

Name:
Name des Berechtigungsprofils, z. B. Schichtarbeiter

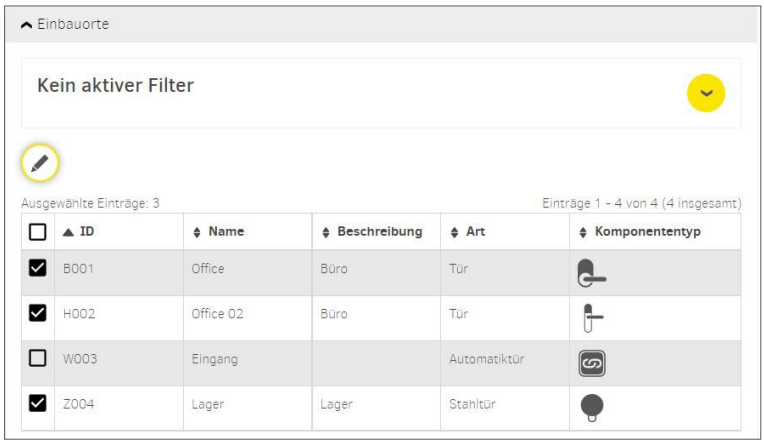
Beschreibung:
Ergänzende Informationen zum Namen, z. B. nur für Schichtarbeiter der Spätschicht

Manual Office-Mode:
Wenn Manual Office-Mode aktiviert ist, haben alle Personen bzw. Zutrittsmedien die Berechtigung, den manuellen Office-Mode an den berechtigten Zutrittskomponenten zu aktivieren.

Standard Zeitprofil:
Auswahl aus den Zeitprofilen

Für das Standard-Zeitprofil dürfen nur Zeitprofile mit maximal 12 Zeitfenstern verwendet werden.

Auswahl der Einbauorte:



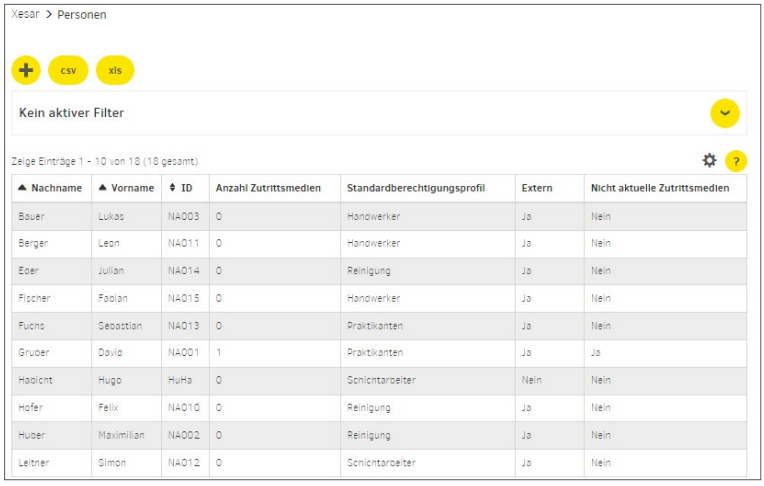
Zutritt zu ausgewählten Einbauorten:

17.10 Personen

Im Bereich Personen werden alle relevanten Informationen der in der Anlage berechtigten Personen definiert. Personen einer Anlage können ein oder mehrere Zutrittsmedien mit unterschiedlichen Berechtigungsprofilen zugewiesen werden.

Personen können auch Benutzer mit entsprechenden Rechten (laut entsprechender Benutzergruppe) sein.

Anzeige Personenliste:



Pflichtfelder sind mit * gekennzeichnet.

Vorname:
Vorname der Person

Nachname:
Nachname der Person

ID:
Kurzzeichen der Person, z. B. Initialen

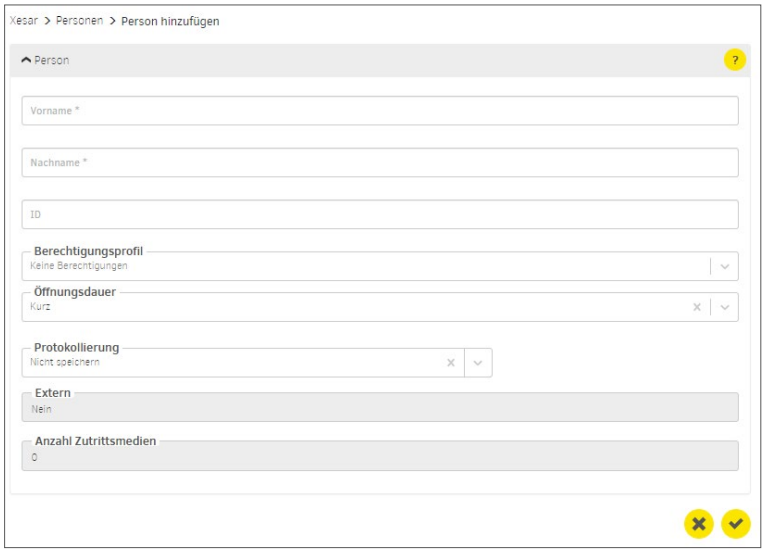
Anzahl der ausgegebenen Zutrittsmedien:
Anzahl der zugewiesenen Zutrittsmedien für die Person

Standardberechtigungsprofil:
Auswahl aus den Berechtigungsprofilen; wird als Standardberechtigungsprofil auf das Zutrittsmedium geschrieben, das der Person zugewiesen ist.

Extern:
Ja – Der Personendatensatz wird von einem Drittsystem über die Drittsystem-Schnittstelle verwaltet.
Nein – Manuelle Verwaltung des Personendatensatzes in der Xesar-Software

Nicht aktuelle Zutrittsmedien:
Ja – Mindestens ein Zutrittsmedium der Person ist nicht aktuell und muss durch Anhalten am Xesar-Online-Wandleser oder Auflegen auf der Codierstation aktualisiert werden.
(Die Darstellung der Statuskachel **Zutrittsmedien nicht aktuell** am Dashboard ist gelb.)
Nein – Alle Zutrittsmedien der Person sind aktuell; Anhalten am Xesar-Online-Wandleser oder Auflegen auf der Codierstation ist nicht notwendig.

17.10.1 Person hinzufügen



Pflichtfelder sind mit * gekennzeichnet.

Vorname:
Vorname der Person

Nachname:
Nachname der Person

ID:
Kurzzeichen der Person, z. B. Initialen

Berechtigungsprofil:
Auswahl aus den Berechtigungsprofilen; wird als Standardberechtigungsprofil auf das Zutrittsmedium geschrieben, das der Person zugewiesen ist.

Öffnungsdauer:
Die Öffnungsdauer ist **Kurz** oder **Lang** und wird bei berechtigtem Zutritt an der Zutrittskomponente aktiviert.

Protokollierung:
Ereignis-Aufzeichnungsart – Zutritte können nicht, unbegrenzt oder zeitlich begrenzt aufgezeichnet werden.

Dauer:
Eingabe der Aufzeichnungsdauer in Tagen, wenn zeitlich begrenzte Aufzeichnung definiert wurde.

Extern:
Ja – Der Personendatensatz wird von einem Drittsystem über die Drittsystem-Schnittstelle verwaltet.
Nein – Manuelle Verwaltung des Personendatensatzes in der Xesar-Software

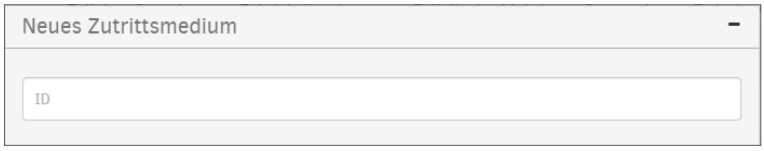
Anzahl der ausgegebenen Zutrittsmedien:
Anzahl der zugewiesenen Zutrittsmedien für die Person

17.11 Zutrittsmedien

Zutrittsmedien dienen zum Öffnen von Türen bei vorhandener Berechtigung sowie zum Transport von anlagenspezifischen Sicherheitsdaten zwischen den Zutrittskomponenten und der Verwaltungssoftware über das virtuelle Netzwerk XVN (Xesar Virtuelles Netzwerk).

17.11.1 Neues Zutrittsmedium

Mit Auflegen eines neuen Zutrittsmediums auf die Codierstation erscheint folgendes Eingabefeld:



ID:
(Identifikator oder Kennzeichen ist kein Pflichtfeld)

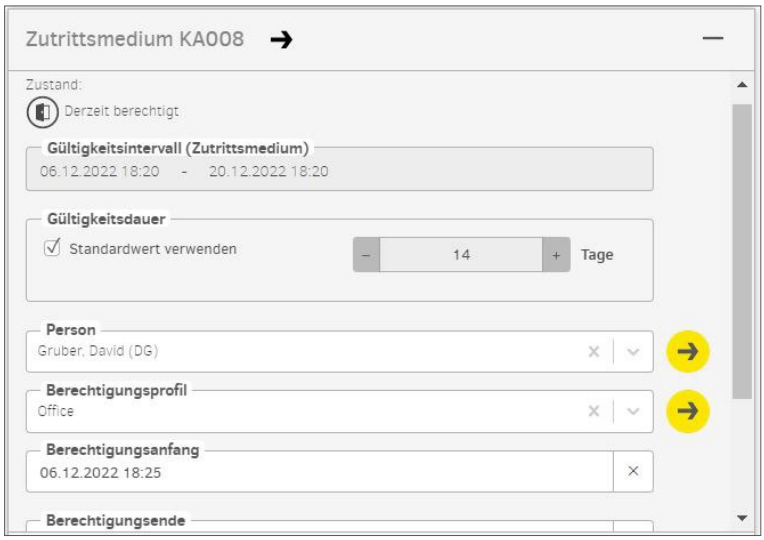
Sie können dem Zutrittsmedium eine Zutrittsmedienbezeichnung (z. B. Hans Huber Garage, Besucher 1 oder Zimmer 23) geben.

Die Vergabe oder Änderung einer ID ist jederzeit in der Zutrittsmedium-Detailansicht in der Xesar-Software möglich.

Das Kennzeichen eines Zutrittsmediums wird nicht anonymisiert, wenn die Zutritte (Personenbezug) nicht aufgezeichnet werden sollen. Das heißt, das Kennzeichen sollte keinen Personenbezug, z. B. Hans Huber, enthalten. Diese Kennzeichnung liegt in der Verantwortung des Benutzers, der die IDs für die Zutrittsmedien vergibt.

Damit in der Ereignisliste die ID des Zutrittsmediums angezeigt wird, muss es einer Person zugeordnet werden. Bei Medien mit Feuerwehr- oder Generalhauptschlüssel-Berechtigung muss, wenn es keiner bestimmten Person zugewiesen werden soll, eine Person „Feuerwehr" oder „Generalhauptschlüssel" angelegt und entsprechend zugewiesen werden.

Nach Bestätigung erscheint eine weitere Seite mit folgenden Anzeige- und Eingabefeldern:



Pflichtfelder sind mit * gekennzeichnet.

Zustand:
Aktuellen Zustand betreffend Gültigkeit und Aktualität.

Gültigkeitsintervall:
Auswahl des Zeitintervalls, bis das Zutrittsmedium wieder am Xesar-Online-Wandleser oder der Codierstation aktualisiert werden muss (Gültigkeit wird verlängert).

Gültigkeitsdauer:
Information des Zeitraums, für den das Zutrittsmedium gültig ist.

- **Standardwert:**
  Wird in den allgemeinen Sicherheitseinstellungen definiert.
- **Individuell:**
  Eingabe 1 Tag bis max. 7300 Tage (ca. 20 Jahre)

Person:
Das Zutrittsmedium kann einer angelegten Person zugewiesen werden. Einer Person können mehrere Zutrittsmedien zugewiesen werden.

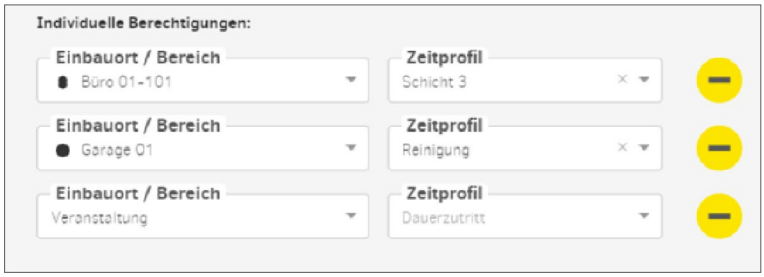
Zutrittsmedium (Ersatzmedium) – Das Feld erscheint nur bei einem neuem Zutrittsmedium:
Zum Erstellen eines Ersatzmediums wird hier das zu ersetzende Zutrittsmedium der oben ausgewählten Person mit seinem Berechtigungsprofil ausgewählt.

Berechtigungsprofil:
Auswahl des gewünschten Berechtigungsprofils

Berechtigungsanfang:
Zeitpunkt für Berechtigungsanfang des Zutrittsmediums. Der Zeitpunkt kann auch in der Zukunft liegen, z. B. bei Hotelbuchungen.

Berechtigungsende:
Der Zeitpunkt für Berechtigungs- und Gültigkeitsende des Zutrittsmediums (z. B. Praktikumsende).
Nach diesem Zeitpunkt kann die Gültigkeit des Zutrittsmediums nicht mehr verlängert werden.

Individuelle Berechtigungen:
Einem Zutrittsmedium können neben einem Berechtigungsprofil noch bis zu 3 zusätzliche individuelle Berechtigungen vergeben werden.
Es können 3 Einbauorte oder Bereiche mit je einem unterschiedlichen Zeitprofil definiert werden.



17.11.2 Vorhandenes Zutrittsmedium

Nach Auflegen eines bestehenden Zutrittsmediums auf die Codierstation wird folgendes Eingabefenster angezeigt:

Zustand des Zutrittsmediums:

#	Zustand	Visualisierung	Erklärung
1	Unsicher gesperrtes Zutrittsmedium		Es gibt noch unsichere Einbauorte
2	Sicher gesperrtes Zutrittsmedium		Es gibt keine unsicheren Einbauorte mehr
3	Unberechtigtes Zutrittsmedium		Das Zutrittsmedium hat keine Berechtigung

#	Zustand	Visualisierung	Erklärung
4	Aktuell gültig		
5	Aktuell ungültig		
6	Aktuell gültiges Zutrittsmedium, das bei Aktualisierung zu einem ungültigen Zutrittsmedium wird		
7	Aktuell ungültiges Zutrittsmedium, das bei Aktualisierung zu einem gültigen Zutrittsmedium wird		
8	Aktuell ungültiges Zutrittsmedium mit einem Gültigkeitsintervall auf dem Zutrittsmedium, das in der Zukunft liegt		
9	Deaktiviertes (gesperrtes) Zutrittsmedium		Das Zutrittsmedium wurde deaktiviert. Es gibt keine unsicheren Einbauorte mehr und der Kalender spielt keine Rolle mehr

Gültigkeitsintervall:
Auswahl des Zeitintervalls, bis das Zutrittsmedium wieder am Xesar-Online-Wandleser oder der Codierstation aktualisiert werden muss (Gültigkeit wird verlängert).

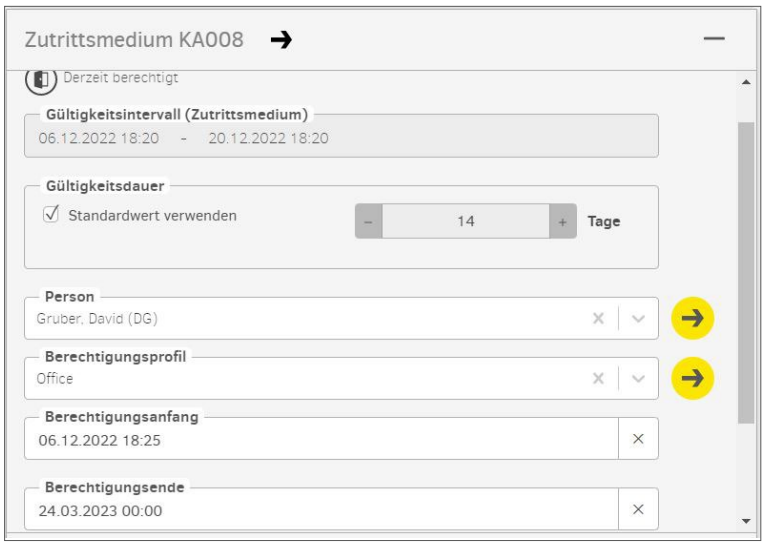
Gültigkeitsdauer:
Information des Zeitraums, für den das Zutrittsmedium gültig ist.

- **Standardwert:**
  Wird in den allgemeinen Sicherheitseinstellungen definiert.
- **Individuell:**
  Eingabe 1 Tag bis max. 7300 Tage (ca. 20 Jahre)

Person:
Person, der dieses Zutrittsmedium zugewiesen ist

Berechtigungsanfang:
Ab diesem Zeitpunkt ist das Zutrittsmedium berechtigt zum Berechtigungsupdate bzw. gültig

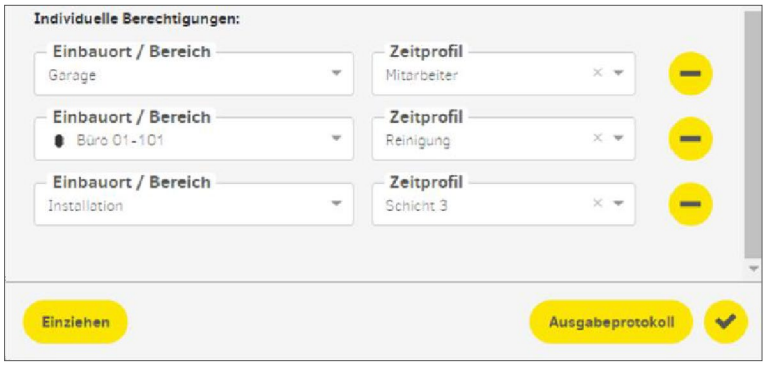
Berechtigungsende:
Ab diesem Zeitpunkt ist das Zutrittsmedium nicht mehr berechtigt zum Berechtigungsupdate bzw. nicht mehr gültig



Individuelle Berechtigungen:
für 3 Einbauorte bzw. Bereiche können dem Zutrittsmedium individuelle Berechtigungen vergeben werden (z. B. für einen persönlichen Garderobenschrank oder Garagenplatz).

Einziehen:
Klicken Sie auf den Button **Einziehen**, wird das Identmedium eingezogen. Alle Einstellungen, bis auf die ID, werden gelöscht. (Die Funktion wird z. B. für Zutrittsmedien von Mitarbeitern verwendet, die das Unternehmen verlassen.)

Zutrittsmedien können wiederverwendet werden. Verwenden Sie daher für die Zutrittsmedien-ID keine personenbezogenen Daten.



Ausgabeprotokoll:
Klicken Sie auf den Button **Ausgabeprotokoll**, wird ein Zutrittsmedien-Ausgabeprotokoll mit allen relevanten Daten als Datei im .pdf-Format generiert. Die pdf-Datei

kann ausgedruckt und bei der Übernahme des Zutrittsmediums vom Empfänger mit seiner Unterschrift bestätigt werden.

Erstellen Sie bei Änderungen der Berechtigungen ein neues Ausgabeprotokoll.

17.11.21, 17:50 Xesar - Fa. EVVA

Xesar

Ausgabeprotokoll

Anlagenname:	Fa. EVVA	
Vorname der Person:	David	
Nachname der Person:	Gruber	
ID Person:	NA001	
ID Zutrittsmedium:	KA008	
Öffnungsdauer:	Kurz	
Protokollierung:	Nicht speichern	
Dauer der Protokollierung:	—	
Berechtigungszeitraum:	29.10.2021 18:10 - ∞	
Gültigkeitsdauer:	14 Tage	
Berechtigungsprofil:	Praktikanten	
Alle Berechtigungen:	**Einbauorte**	**Zeitprofil**
	Bereiche	**Zeitprofil**
	Installation	—
Individuelle Berechtigungen:	**Einbauort / Bereich**	**Zeitprofil**
	Büro 1	—
	Fertigung 2	—
Datum Ausgabe:	29.10.2021 20:14	
Ausgegeben von:	Helmut	

Ausgabe:

Unterschrift

Einzug:

Unterschrift

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

17.12 Zutrittskomponenten hinzufügen

Die Zutrittskomponenten werden im Baustellenmodus ausgeliefert. Zur Funktion in der Xesar-Anlage muss die Zutrittskomponente der Anlage hinzugefügt werden.

Nach der Definition des Einbauortes in der Xesar-Software ist die Zutrittskomponente zum Hinzufügen in die Anlage vorbereitet.

ID	Name	Beschreibung	Art	Kompone...	Zustand im Lebenszyklus
ID001	Eingang 1	Haupteingang Wi...	Automatik Tür		Zum Hinzufügen vorbereitet
ID002	Eingang 2	Nebeneingang Sei...	Glastür		Zum Hinzufügen vorbereitet
ID003	Büro 1	Büro 1	Tür		Zum Hinzufügen vorbereitet

Zum Hinzufügen einer Zutrittskomponente wird in der Xesar-Software eine Konfigurationsaufgabe generiert.

Diese wird auf das Xesar-Tablet synchronisiert und ab Xesar 3.1 vom Xesar-Tablet mittels drahtloser Synchronisation an der G2.1-Zutrittskomponente ausgeführt. Bei älteren Zutrittskomponenten wird die Synchronisation mittels Anschlusskabel durchgeführt.

18 Xesar-System- und Anlagenverwaltung

Die Xesar-Software besteht aus dem Installation-Manager und weiteren Software-Applikationen, wie dem Periphery-Manager.

Der Installation-Manager installiert und verwaltet systemrelevante Einstellungen der Xesar-Anlagen.

Der Periphery-Manager ermöglicht die Anbindung und Verwendung von externen Komponenten, wie z. B. der Codierstation.

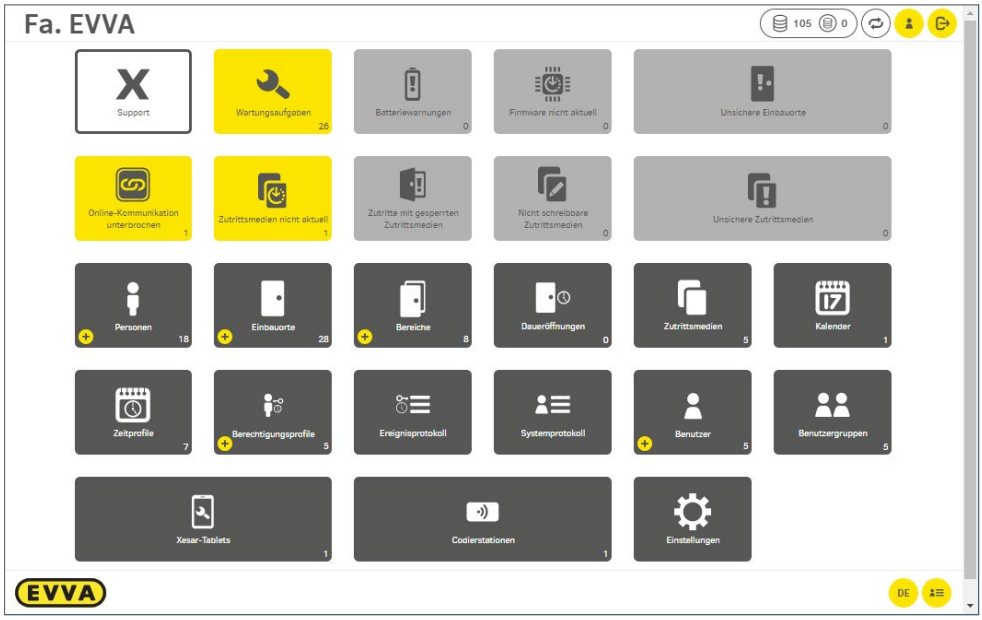
Die Verwaltung der Xesar-Anlage erfolgt auf der Verwaltungsoberfläche (Dashboard) im jeweiligen Browser.

Das Dashboard gibt einen Überblick über den aktuellen Sicherheitszustand der Xesar-Anlage und die notwendigen Wartungsaufgaben.

18.1 Das Dashboard

Das Dashboard bietet eine übersichtliche Darstellung der Funktionen von Xesar.

Das Dashboard ist der Arbeitsplatz, auf dem Zutritsmedien, Personen, Türen, Bereiche und Berechtigungen verwaltet werden. Zusätzlich werden auf dem Dashboard Warnungen, wie unsichere Zutrittsmedien und Einbauorte sowie Hinweise, wie Wartungsaufgaben (Batteriestatus und Firmwarestatus) angezeigt.



Das Dashboard setzt sich aus Kacheln (Felder) zusammen, deren Farben verschiedene Funktionen signalisieren:

- Dunkelgraue Kacheln dienen zur Verwaltung, wie z. B. Erstellung von Bereichen, Einbauorten oder Berechtigungsprofilen.
- Hellgraue Kacheln bedeuten, dass keine Aktionen gesetzt werden müssen.
- Gelbe Kacheln zeigen Warnungen oder Hinweise an. Sobald die damit verbundenen Aufgaben gelöst sind, werden die Kacheln wieder hellgrau.
- In der weißen Kachel Support befinden sich nützliche Downloads, wie Unterlagen (z. B. das Systemhandbuch) oder Dateien für den Austausch mit dem EVVA Technischen Büro Ihres Landes.

18.2 Die Listen-Filterfunktion

Für eine detaillierte Auswertung oder eine vereinfachte Darstellung werden Listen nach einem oder mehreren Kriterien gefiltert.

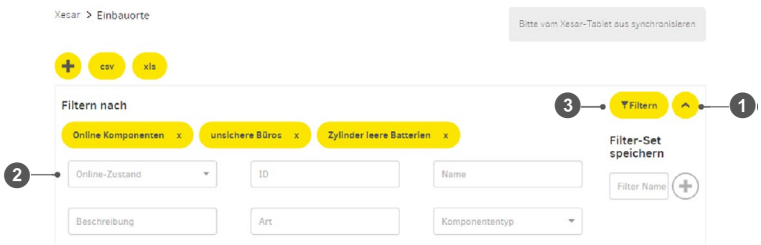
Filtereinstellungen, die Sie häufig benötigen, können als Preset gespeichert werden.

18.2.1 Manuell filtern

» Klicken Sie auf das Symbol **Filterbereich öffnen** ❶

» Wählen Sie die gewünschten Filterkriterien aus ❷

» Klicken Sie auf **Filtern** ❸



18.2.2 Filter-Presets

» Klicken Sie auf das Symbol **Filterbereich öffnen** ❶

» Wählen Sie die gewünschten Filterkriterien aus ❷

» Vergeben Sie einen Namen für Ihr Filter-Preset ❸

» Klicken Sie auf das Symbol **Hinzufügen** ❹

» Klicken Sie auf das Symbol **x** ❺ im Button Feld, um das Preset zu löschen.

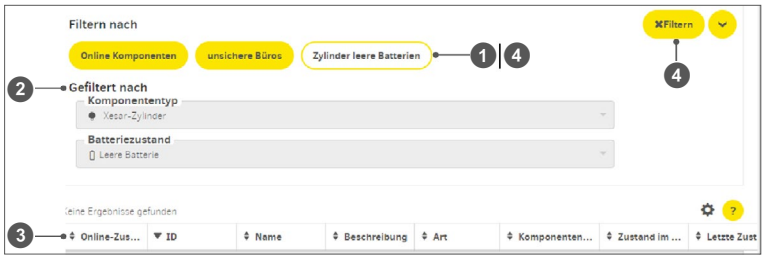
Filter-Preset anwenden:

» Klicken Sie zum Aktivieren auf den Button für das **Filter-Preset** ❶ | ❹

Die Filterkriterien ❷ werden angezeigt

Die Filterergebnisse ❸ werden in der Liste angezeigt

» Klicken Sie nochmals auf den Button für das Filter-Preset ❶ | ❹ oder auf den Button **Filtern** ❹, um die Funktion Filter zu beenden.



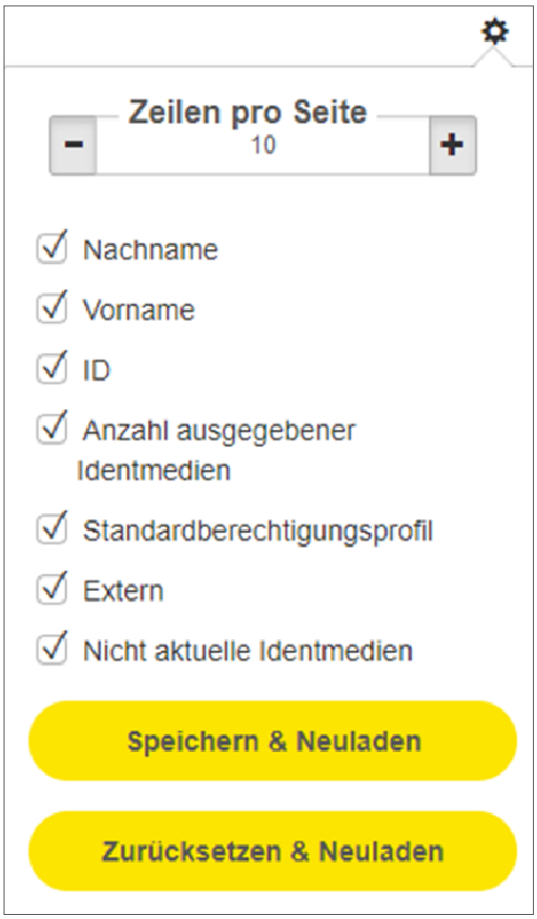
Die Anzahl der Filter-Presets je Liste ist nicht beschränkt.

18.2.3 Spaltenansicht

Die Listenansicht kann nach Bedarf und Größe des Bildschirms angepasst werden.

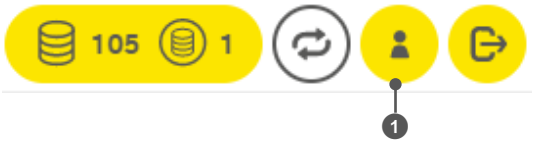
» Klicken Sie auf das Symbol ⚙, um das Fenster für die Auswahl der ein- und auszublendenden Spalten zu öffnen. Zusätzlich stellen Sie im Auswahlfenster die Anzahl der maximal angezeigten Zeilen pro Seite ein.

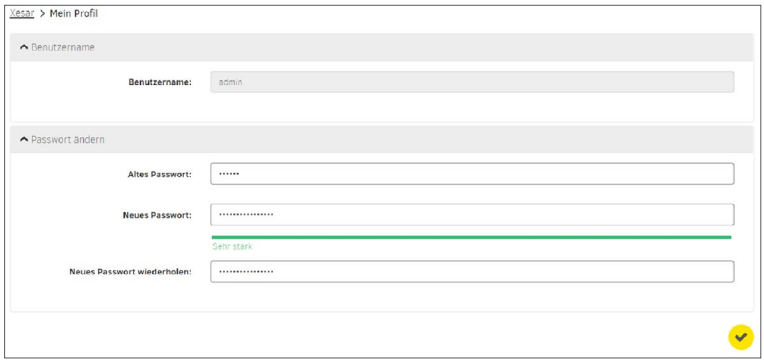
Die vorgenommenen Einstellungen können gespeichert bzw. wieder zurückgesetzt werden. Die gespeicherten Einstellungen bleiben für alle Listen – auch nach Verlassen der Seite – beim jeweiligen Benutzer erhalten



18.3 Mein Profil

Der Menüpunkt **Mein Profil** ❶ befindet sich in der oberen rechten Ecke des Dashboards. (Alternativ gelangen Sie über das Feld **Benutzer** und Auswahl des Benutzerkontos zur Seite **Mein Profil**.)





Mein Profil gibt direkten Aufschluss darüber, welcher Benutzer gerade angemeldet ist (Benutzername) und die Anlage verwaltet.

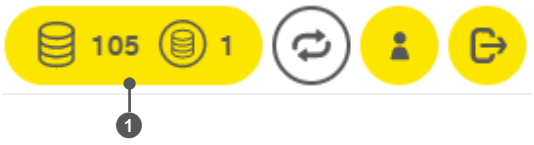
Im Bereich **Mein Profil** können Änderungen des Benutzernamens und des Passwortes vorgenommen werden. Bei einer Passwortänderung wird automatisch eine Bewertung des Sicherheitsgrades des Passwortes angezeigt. Das Spektrum reicht von sehr schwach (rot) bis sehr stark (grün).

18.4 KeyCredits (Stück)

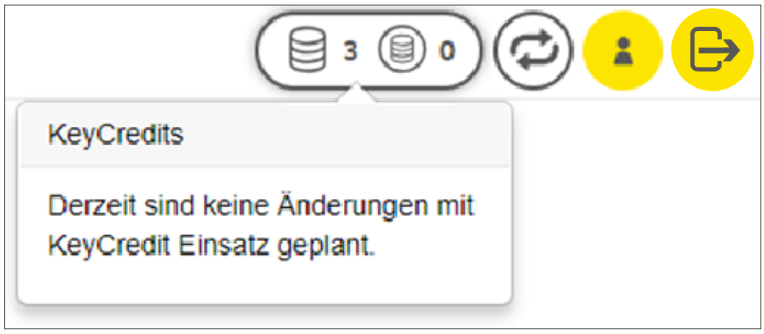
Am Dashboard wird das aktuelle Guthaben und abzubuchende KeyCredits ❶ angezeigt.

Kostenpflichte Änderungen betreffen

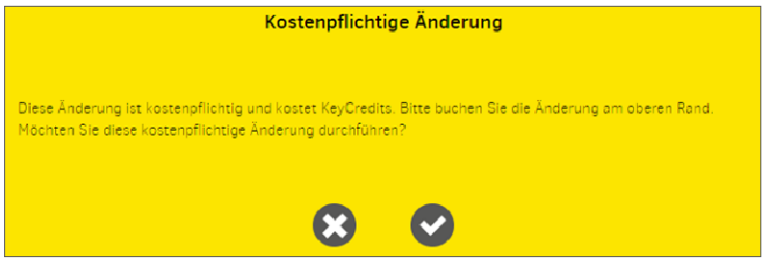
- Neuausstellung von Zutrittsmedien
- Berechtigungsveränderungen



Sperren oder der Entzug von Berechtigungen ist kostenlos.

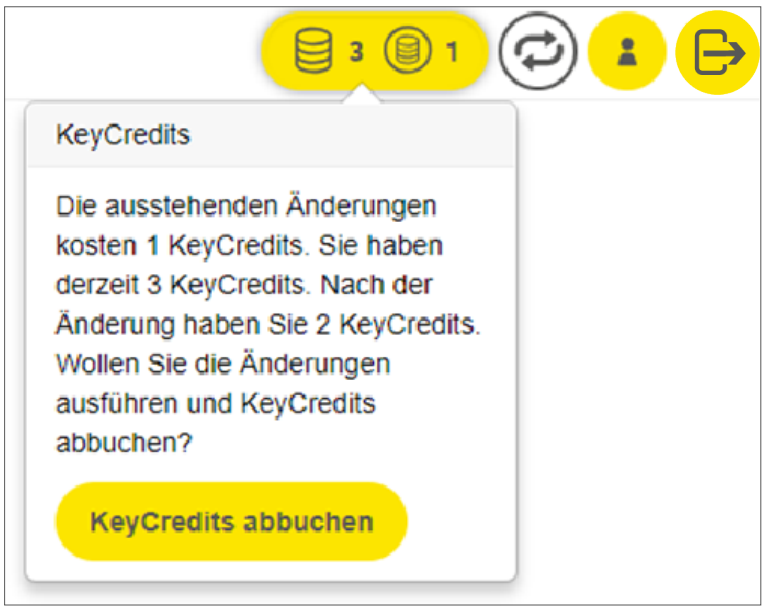


Kostenpflichte Änderungen werden direkt bei der Erstellung oder Änderung von Berechtigungen am Zugriffsmedium angezeigt.



» Bestätigen Sie die Meldungen.
Sie können weitere Berechtigungsänderungen durchführen und abschließend alle Änderungen für die KeyCredits-Abbuchung bestätigen.

Die Information zu Ihren KeyCredits ist Sie am Dashboard.

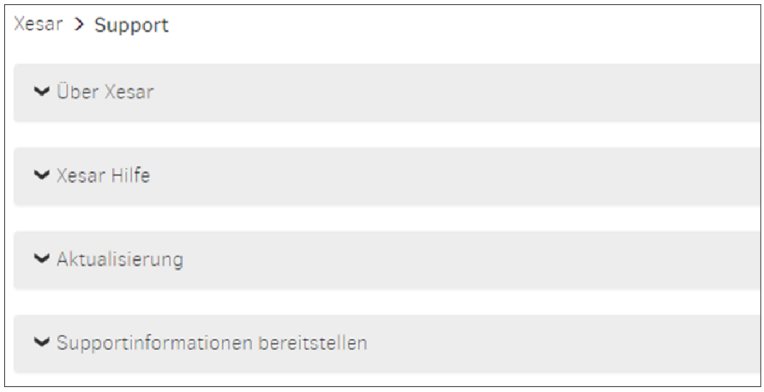


Bei KeyCredit Xesar Lifetime sind alle Berechtigungsänderungen und Ausstellungen von Zugriffsmedien inkludiert und müssen nicht bestätigt werden.

Beachten Sie die Informationen zum Aufladen der KeyCredits im Kapitel „Installation-Manager".

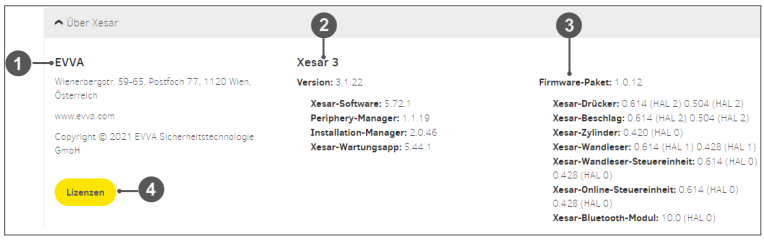
18.5 Support

Auf der Support-Seite werden folgende Support-Optionen angeboten:



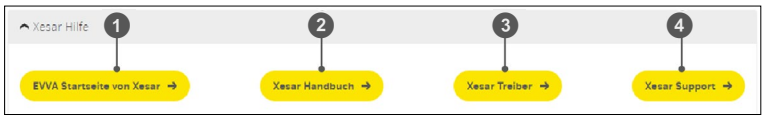
18.5.1 Über Xesar

- EVVA Impressum ❶
- Installierte Xesar-Version mit den Versionen des Installation-Managers, Periphery-Managers und Xesar-Wartungsapp ❷
- Ausgelieferte Firmware-Versionen der Zutrittskomponenten ❸
- Link zu den Allgemeinen Lizenzbedingungen von EVVA (mit Download-Möglichkeit) ❹



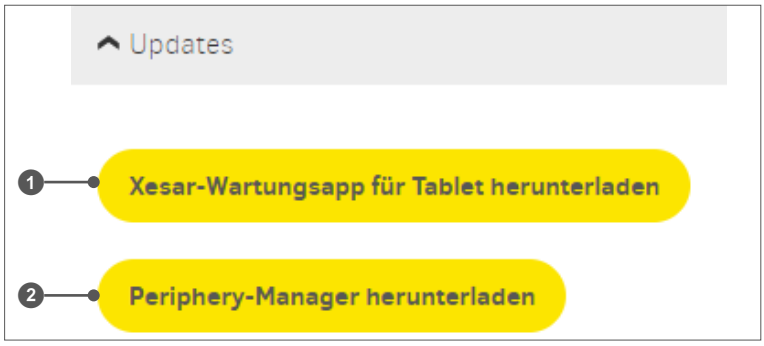
18.5.2 Xesar-Hilfe

- Link zur Xesar-Produktseite auf der EVVA-Website ❶
- Link zum Xesar-Systemhandbuch auf der Xesar-Produkt Download-Seite ❷
- Link zur Xesar-Produktseite mit Information zum Treiber-Download für die Codierstation ❸
- Link zur Xesar-Supportseite von EVVA ❹



18.5.3 Updates

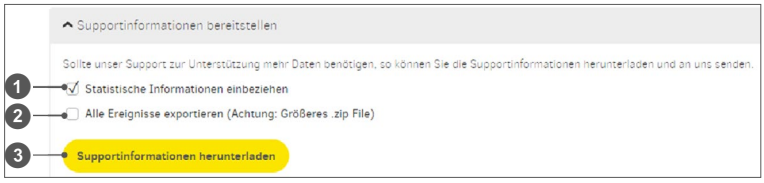
- Download der aktuellen Xesar-Wartungsapp ❶
- Download des aktuellen Periphery-Managers ❷



18.5.4 Supportinformationen herunterladen

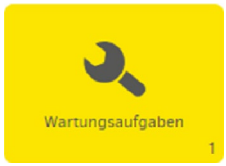
Sie können bestimmen, welche Supportinformationen zusammengefasst werden.

- Statistische Informationen einbeziehen (z. B. Anzahl von Einbauorten, Bereichen, Personen, Identmedien, gesperrten Zutrittsmedien oder Einbauorte pro Bereich) ❶
- Alle oder limitierte Anzahl der Ereignisse ❷
- Download der Supportinformationen ❸



Bei Bedarf laden Sie die Supportinformationen herunter. Die anonymisierten Anlagendaten werden für die Fehleranalyse benötigt. Senden Sie die Daten nach Rücksprache an das EVVA Technische Büro.

19 Wartungs- und Konfigurationsaufgaben



Wartungsaufgaben sind Konfigurations- und Wartungsaufträge für Zutrittskomponenten, wie

- Hinzufügen
- Konfigurieren
- Firmware-Update
- Entfernen

Die Kachel **Wartungsaufgaben** ist gelb, wenn eine neue Aufgabe vorhanden ist. Diese wird automatisch vom System erstellt, sobald eine Zutrittskomponente gewartet werden muss.

Die Wartungsaufgaben werden mit dem Xesar-Tablet an den Zutrittskomponenten ausgeführt!

Der Benutzer mit der entsprechenden Benutzergruppen-Berechtigung kann die Wartungsaufgaben (alle oder nach Bereichen) auf dem Xesar-Tablet synchronisieren. Dazu benötigt er keine Zutrittsberechtigung zu den betroffenen Einbauorten.

Arbeitstechnisch ist es jedoch von Vorteil, wenn der Wartungstechniker die Zutrittsberechtigungen zu den betroffenen Einbauorten hat. Dafür muss ihm ein Zutrittsmedium mit den entsprechenden Zutrittsberechtigungen übergeben werden.

Software-Updates können auch durchgeführt werden, wenn offene Wartungsaufgaben vorhanden sind.
(Bei Upgrades von Xesar 2.2 auf Xesar 3.x dürfen keine Wartungsaufgaben offen sein.)

19.1 Firmware-Update

Die Kachel **Firmware nicht aktuell** ist hellgrau, wenn keine Aufgaben offen sind. Gegebenfalls wird sie gelb und zeigt an, bei welchen Zutrittskomponenten die Firmware aktualisiert werden soll. Ein Update der Firmware bietet folgende Vorteile:

- Mögliche Fehler wurden behoben
- Die Batterielebensdauer wurde durch Anpassungen erhöht
- Neue Funktionen sind hinzugefügt worden

Es wird automatisch eine Wartungsaufgabe kreiert, falls eine Zutrittskomponente nicht über die aktuelle Firmware verfügt.

Ein Firmware-Update kann auch ohne Hinzufügen einer Zutrittskomponente in eine Anlage erfolgen.

19.2 Batteriewarnung

Die Kachel **Batteriewarnungen** wird gelb und zeigt alle Zutrittskomponenten an, bei denen die Batterie leer ist und ersetzt werden soll.

Wenn die Batteriespannung einer Komponente unter den definierten Wert fällt, wird in der Komponente die Information „Batterie leer" ausgelöst und durch ein optisches und akustisches Signal angezeigt.

Nach dem erstmaligen Anzeigen der Batteriewarnung an der Komponente sind noch bis zu 1000 Öffnungen möglich.

Die Information „Batterie Leer" wird mittels XVN über die Medien oder mit dem Xesar-Tablet in die Software übertragen. Am Dashboard wird die „Batteriewarnung" an der

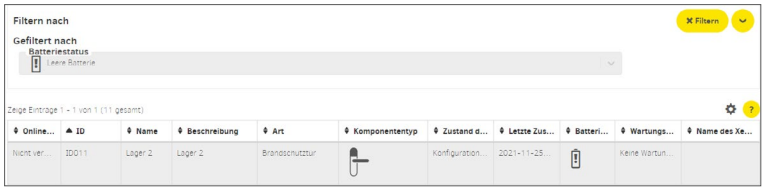
gelben Kachel „Batteriewarnungen“ angezeigt. Ein Klick auf die gelbe Kachel zeigt alle Komponenten mit Batteriewarnung an.

» Führen Sie die Wartungsaufgabe aus und

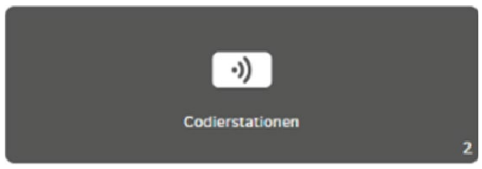
» tauschen Sie möglichst bald die Batterien.

Nach dem Batterietausch verbinden Sie die Komponente mit dem Xesar-Tablet und synchronisieren Sie das Xesar-Tablet mit der Software. Damit wird die Batteriewarnung in der Software zurückgesetzt.

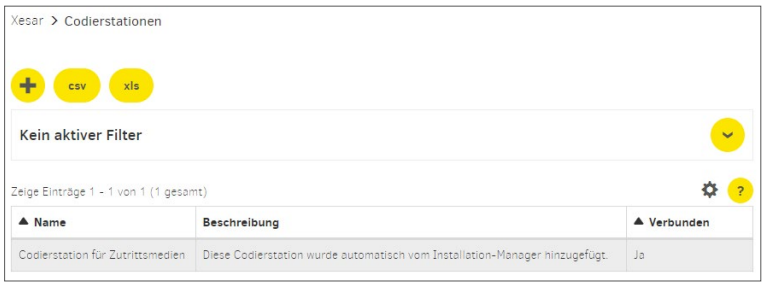
Für alle betroffenen Zutrittskomponenten wird eine Wartungsaufgabe erstellt.

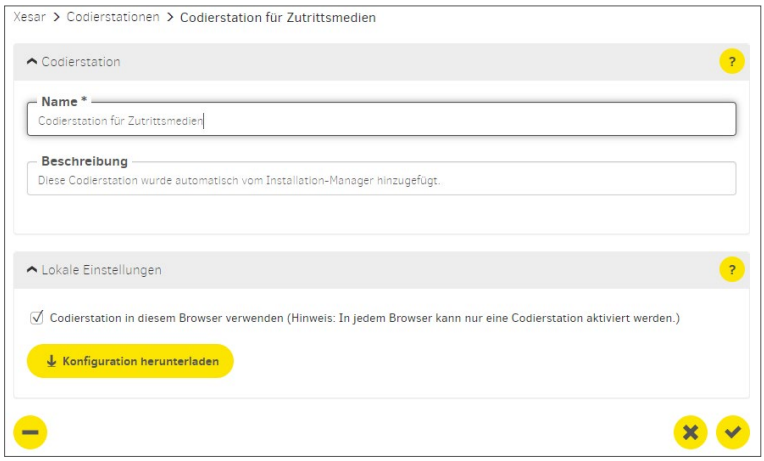


19.3 Codierstationen



In der Kachel **Codierstationen** sind alle aktiven und inaktiven verwendeten Codierstationen aufgeführt.





Bei der Installation von PC-Anlagen wird die Codierstation des Admin-PCs automatisch durch den Installation-Manager hinzugefügt. Die Verwaltung der Codierstation am Admin-PC erfolgt über die Konfigurationsseite der Anlage im Installation-Mananger. Siehe Kapitel „Xesar Installation"

Für den Anschluss von Codierstationen an Client-PCs ist die Installation des Periphery-Managers am Client-PC notwendig.

Sie benötigen eine aktive Codierstation, um Zutrittsmedien auszustellen oder updaten zu können.

Installieren und konfigurieren Sie den Periphery-Manager, um die Xesar-Software und Ihre Anlage mit der Codierstation zu verbinden. (Siehe Kapitel „Codierstation mit der Xesar-Software verknüpfen".)

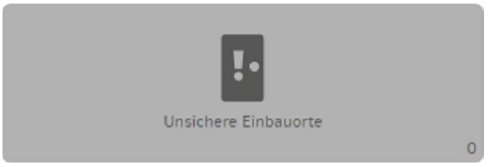
19.4 Online-Störung

Die Kachel **Online Störung** wird gelb, wenn eine Online-Störung auftritt. Wenn der Xesar-Online-Wandleser nicht mit der Xesar-Software verbunden ist, können keine Zutrittsmedien an diesem Xesar-Online-Wandleser aktualisiert werden. Der Wandleser funktioniert jedoch wie ein Offline-Wandleser.

Bitte prüfen Sie, ob

- Ihr Xesar-Netzwerkadapter richtig eingestellt ist
- Die Xesar-Steuereinheit richtig mit dem Xesar-Netzwerkadapter verbunden ist

19.4.1 Unsichere Einbauorte

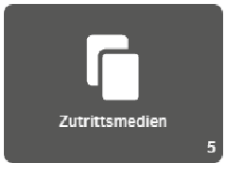


Die Kachel **Unsichere Einbauorte** wird gelb, wenn ein Zutrittsmedium gesperrt wurde und die Blacklist an den Einbauorten nicht aktuell ist.

Die Blacklist-Aktualisierung kann durch das XVN oder durch eine Synchronisation zwischen der Xesar-Software und der Zutrittskomponente mit dem Xesar-Tablet erfolgen.

Es wird automatisch eine Wartungsaufgabe erzeugt, sobald ein unsicherer Einbauort existiert.

19.5 Zutrittsmedien

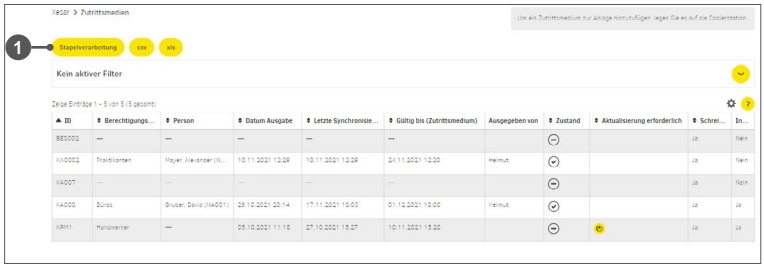


Für Xesar stehen verschiedene Formen von Zutrittsmedien zur Verfügung (siehe Kapitel „Zutrittsmedien“).

Die Anzahl der angezeigten Zutrittsmedien ist die Anzahl aller Zutrittsmedien der Anlage, unabhängig davon, ob sie z. B. gesperrt oder unbeschrieben sind. Zutrittsmedien können nicht aus der Liste gelöscht werden.

19.5.1 Zutrittsmedien – Stapelverarbeitung

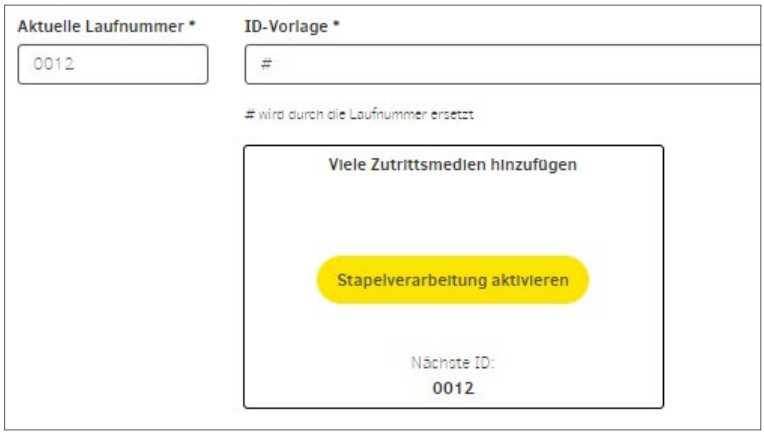
In Xesar gibt es mit der Stapelverarbeitung die Funktion, schnell und einfach mehrere Zutrittsmedien zur Xesar-Anlage hinzuzufügen. Die Funktion Stapelverarbeitung ist in der Kachel Zutrittsmedien im Menüpunkt **Stapelverarbeitung** ❶



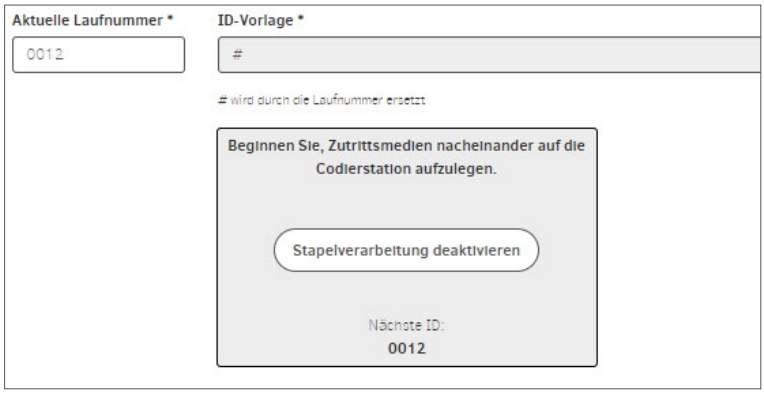
Um mit der Stapelverarbeitung zu beginnen, geben Sie die aktuelle Laufnummer-ID ein, um den Zutrittsmedien eine fortlaufende Nummer in der Xesar-Software zuzuteilen. Wenn Sie keine Nummer vergeben, verwendet das Xesar-System den Defaultwert und vergibt die Nummern selbstständig.

» Klicken Sie auf **Stapelverarbeitung aktivieren** und legen Sie das erste Zutrittsmedium auf die Codierstation.

ID ist z. B. die Personalnummer.

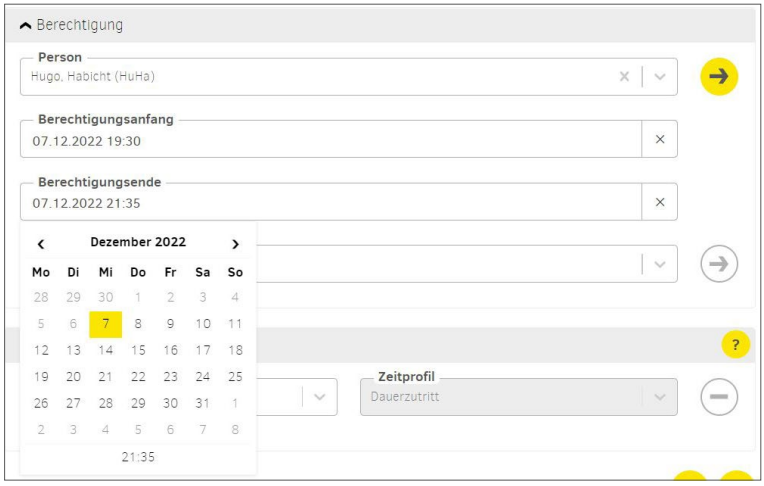


Über **Stapelverarbeitung deaktivieren** wird die Stapelverarbeitung gestoppt.



19.5.2 Zutrittsmedien inaktiv setzen

Wenn die Zutrittsberechtigung einer Person für längere Zeit unterbrochen werden soll, kann das Zutrittsmedium deaktiviert werden. Dabei bleibt das Medium mit dem Berechtigungsprofil der Person zugewiesen. Der Zutritt wird durch Setzen des Berechtigungsende auf den aktuellen Zeitpunkt bis auf weiteres deaktiviert.



- Öffnen Sie die Detailseite des Zutrittsmediums, das inaktiv gesetzt werden soll.
- Klicken Sie auf das aktuelle Berechtigungsende (Datum mit Uhrzeit, z. B.7.12. um 21:35). Das Medium wird sofort inaktiv gesetzt.
- Anschließend aktualisieren Sie das Medium am Online-Wandleser oder an der Codierstation, damit es zur Anlage keinen Zutritt mehr hat.

Die Zutrittsberechtigung am Medium kann durch Setzen eines neuen Berechtigungsende-Zeitpunkts und Aktualisierung am Online-Wandleser oder an der Codierstation wieder aktiviert werden.

Bei diesem Vorgang werden keine Blacklisteinträge in der Anlage erzeugt.

19.5.3 Zutrittsmedien einziehen

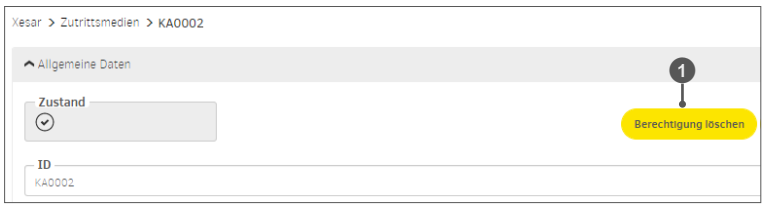
Ein Zutrittsmedium kann nur eingezogen werden, wenn es auf der Codierstation liegt. Nur dann ist der Button **Einziehen** sichtbar. Bei diesem Vorgang werden die gespeicherten Daten auf dem Zutrittsmedium gelöscht; es kann wieder neu beschrieben werden.

Das Zutrittsmedium bleibt in der Liste der Zutrittsmedien erhalten.

Das Einziehen eines Zutrittsmediums löscht alle Daten, außer dem Schlüssel der Installation im Speicher.

19.5.4 Zutrittsmedium Berechtigung löschen

Für nicht kritische Zutrittsmedien (z B. Zutrittsmedien von Personen, die keinen Zugang mehr haben sollen, z. B. Fremdfirmen im Gebäude) gibt es die Funktion **Berechtigung löschen** ❶. Beim Löschen einer Berechtigung eines Zutrittsmediums wird kein Blacklisteintrag erstellt und am Dashboard wird keine Warnmeldung angezeigt.



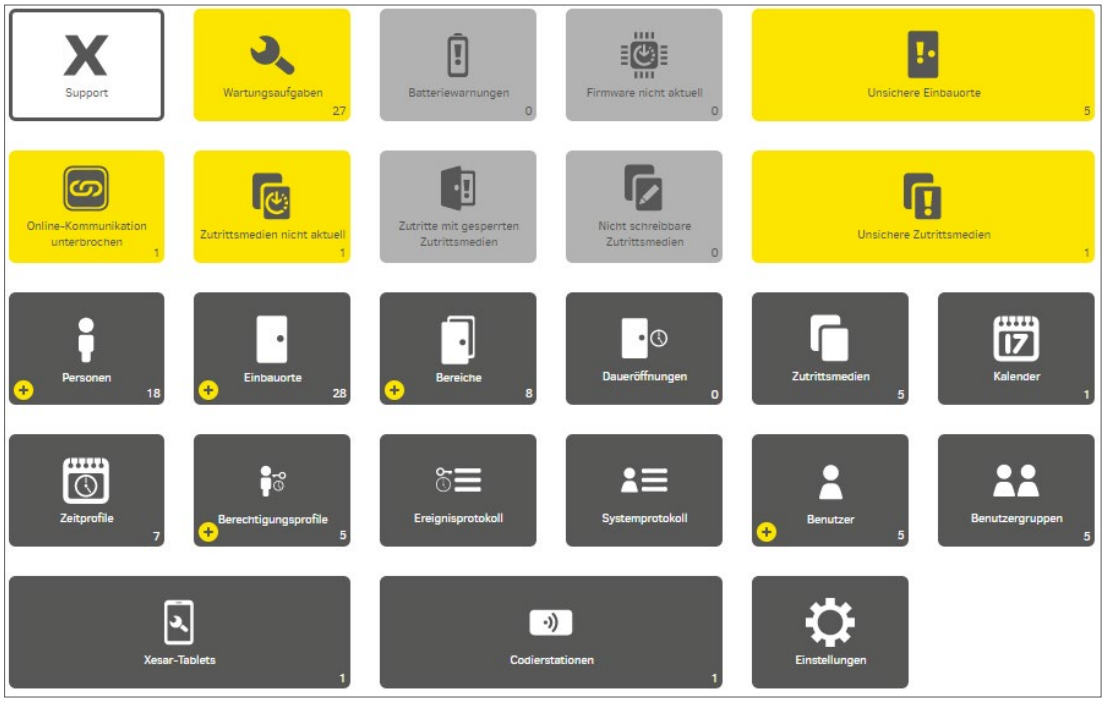
» Klicken Sie am Dashboard auf den Menüpunkt **Zutrittsmedien** und wählen Sie das betroffene Zutrittsmedium aus.

19.5.5 Zutrittsmedium sperren (auf Blacklist setzen)

Ein Zutrittsmedium, das Sie sperren ❶ wird automatisch auf eine Blacklist gesetzt. Die Blacklist gilt als Sicherheitsrisiko-Liste. Personen mit gesperrten Zutrittsmedien haben solange Zutritt, bis jede einzelne betroffene Zutrittskomponente aktualisiert wurde. Das kann entweder über Wartungsaufgaben mit dem Xesar-Tablet oder über das XVN (Xesar Virtuelles Netzwerk) erfolgen.

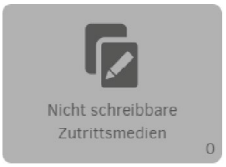
Am schnellsten wird die Anlage via XVN gesichert.

Im Dashboard der Xesar-Software werden noch nicht aktualisierte Einbauorte signalisiert. Es wird für jeden Einbauort eine Wartungsaufgabe kreiert sowie die Felder **Unsichere Einbauorte** und **Unsichere Zutrittsmedien** ändern ihre Farbe auf gelb.



19.5.6 Nicht schreibbare Zutrittsmedien

Die Kachel **Nicht schreibbare Zutrittsmedien** signalisiert, dass bei bestimmten Zutrittsmedien der interne Kartenspeicher (Aktuell: 4k Bytes) voll beschrieben ist. Die Kachel ist gelb – eine Sicherheitsvorkehrung, falls sich nicht schreibbare Zutrittsmedien im Umlauf befinden. Rechts wird die Anzahl der nicht schreibbaren Zutrittsmedien angezeigt.



Das Xesar-Segment auf dem Zutrittsmedium benötigt etwa 2 KB.

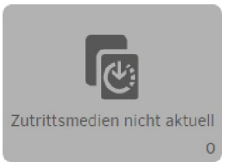
Falls die für Xesar freigegebene Speicherkapazität des Zutrittsmediums überschritten wird, färbt sich das Feld gelb. Einem Zutrittsmedium können maximal 96 Bereiche oder 32 Einbauorte zugewiesen werden. Sollte eine Erweiterung der Berechtigung des Zutrittsmediums durchgeführt werden, wird eine Warnung angezeigt.

Zusammenfassen von Bereichen erhöht die Speicherkapazität des Zutrittsmediums.

19.5.7 Unsichere Zutrittsmedien

Unsichere Zutrittsmedien entstehen durch das Sperren von Zutrittsmedien. In diesem Zustand kann das gesperrte Zutrittsmedium trotzdem noch Zutrittskomponenten öffnen (siehe Kapitel „Identmedium sperren (auf die Blacklist setzen)“).

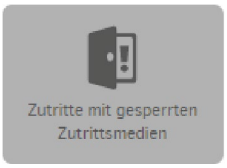
19.5.8 Zutrittsmedien nicht aktuell



Nach bestimmten Funktionen, z. B. nach einer Berechtigungsänderung müssen Zutrittsmedien aktualisiert werden. Das Feld färbt sich gelb und zeigt somit an, dass Zutrittsmedien nicht aktuell sind und aktualisiert werden müssen.

Zutrittsmedien können an der Codierstation oder am Xesar-Online-Wandleser aktualisiert werden.

19.5.9 Zutritte mit gesperrten Zutrittsmedien



Die Kachel **Zutritte mit gesperrten Zutrittsmedien** zeigt an, ob und wo Zutritte mit gesperrten Zutrittsmedien erfolgt sind.

Halten Sie die Anlage mit Wartungsaufgaben und XVN-Funktionalität aktuell.

19.6 Protokolle

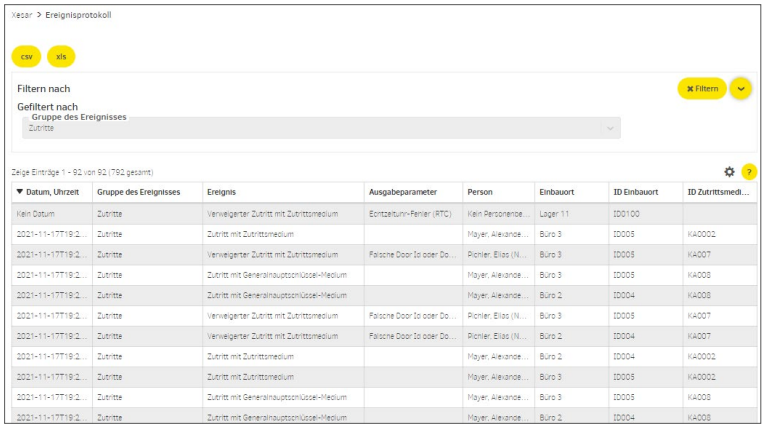
In Xesar werden zwei Arten von Protokollen unterschieden:

- Ereignisprotokoll
- Systemprotokoll

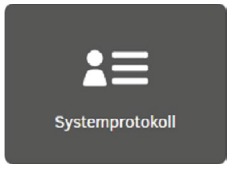
19.6.1 Ereignisprotokoll

Das Ereignisprotokoll zeigt die Log-Einträge von Ereignissen an, die durch die Interaktion mit dem elektromechanischen Schließsystem (z. B. Zutritte oder Abweisungen an den Zutrittskomponenten) ausgelöst werden.

Die Ereignisprotokollierung ist abhängig von den Einstellungen zum Personenbezug unter Einstellungen sowie von den jeweiligen Protokollierungseinstellungen an den Zutrittskomponenten, unter Einbauorte und Protokollierungseinstellungen bei den einzelnen Personen.



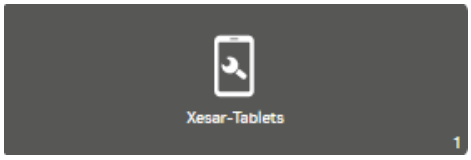
19.6.2 Systemprotokoll



Das Systemprotokoll dokumentiert alle Aktionen, die von den Benutzern ausgeführt werden. Das heißt, es erfasst Ereignisse, die durch Verwaltungsaufgaben ausgelöst werden. Es erfasst im Gegensatz zum Ereignisprotokoll keine Ereignisse, die aus der Interaktion mit dem elektromechanischen Zutrittssystem ausgelöst werden.

» Klicken Sie auf den Button , um den Einbauort direkt aufzurufen und Änderungen vornehmen.

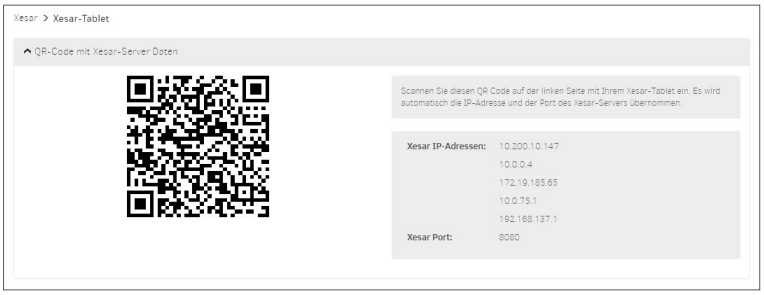
19.7 Xesar-Tablets (Wartungsgeräte)



In der Ansicht „Xesar-Tablets" werden alle mit der Anlage verbundenen Wartungsgeräte angezeigt.

QR-Code in Listenansicht für Anlagen IP und Port:

» Scannen Sie diesen QR-Code mit Ihrem Xesar-Tablet ein. Die IP-Adresse und der Port der Anlage werden automatisch übernommen.



» Klicken Sie auf den Button **Verlust melden** ❶, um das Xesar-Tablet aus der Anlage zu nehmen.

Weitere Informationen siehe Kapitel „Xesar-Wartungsapp".

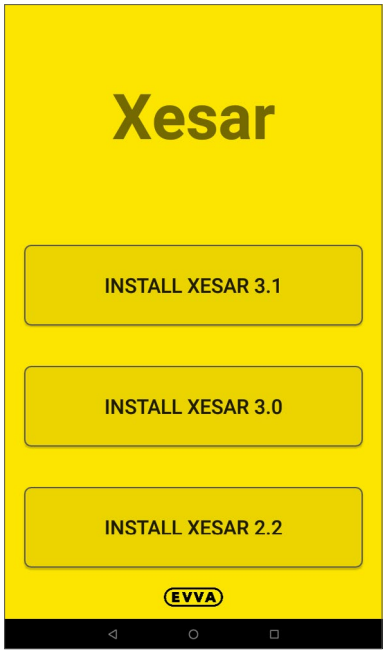
20 Xesar-Wartungsapp

Diese Anleitung beschreibt die Bedienung der Xesar-Wartungsapp am Tablet ARES BLE 4.2. für die Konfiguration von Xesar-Zutrittskomponenten mit Bluetooth Low Energy Kommunikationsschnittstelle, als auch älteren Zutrittskomponenten mit USB-Schnittstelle.

Wenn die Xesar-Wartungsapp auf einem älteren Tablet als ARES BLE 4.2 betrieben wird, ist die Bedienoberfläche abweichend. (Siehe Kapitel „Bedienung der Xesar-Wartungsapp auf älteren Xesar-Tablets“.)

20.1 Xesar-Wartungsapp starten

Nach dem Einschalten eines neuen Tablets erscheint der Startbildschirm. mit der Auswahl für die gewünschte App für Xesar 2.2- oder Xesar 3.x-Anlagen.



» Wählen Sie die entspechende Xesar-Wartungsapp der Xesar-Version Ihrer Anlage.

» Ab Xesar 3.1:
Stellen Sie sicher, dass Bluetooth und die Standortabfrage auf Ihrem Tablet sowie die Xesar-Wartungsapp aktiviert und zugelassen sind. Weiters muss sich das Tablet im gemeinsamen WLAN mit dem Anlagen-PC befinden.

» Wischen Sie mit einem Finger am Bildschirm von unten nach oben, um zu der Ansicht aller installierten Apps am Tablet zu gelangen.

» Klicken Sie auf das Xesar-Icon , um die Xesar-Wartungsapp zu starten.

Die Startseite der Xesar-Wartungsapp beinhaltet folgende Bedien- und Anzeigebereiche:

- Kopfzeile:
  - Filterbutton
  - Einstellungen
  - Button zum Abmelden (Logout)
- Informationszeile
- Reiterzeile der beiden Ansichtsseiten
  - Liste der Zutrittskomponenten in Reichweite
  - Liste der Wartungsaufgaben
- Anzeige- und Funktionsfeld
- Button zum Synchronisieren mit der Xesar-Software

Gelbe Buttons sind empfohlene aktionierbare Buttons.
Weiße Buttons sind mögliche aktionierbare Buttons.
Graue Buttons sind deaktivierte Buttons.

20.2 Tablet mit der Xesar-Software verbinden

Um Wartungsaufgaben durchführen zu können, muss das Tablet mit der Xesar-Software verbunden werden.

» Drücken Sie den Button **Synchronisation mit Xesar-Software**. Sie gelangen zur Login-Seite.

Für einen erfolgreichen Login sind folgende Eingaben erforderlich:

- **Name**:
  Xesar-Tablet (voreingestellt)
  Der Name ist frei wählbar, maximal 50 Zeichen.
- **Benutzername** und **Passwort**:
  Zugangsdaten des Benutzers in der Xesar-Software.

Zur Verbindung des Tablets mit der Anlage müssen sich beide im selben WLAN befinden

Bei der Verwendung von mehreren Tablets in einer Anlage, muss jedes Tablet einen eigenen Namen haben.

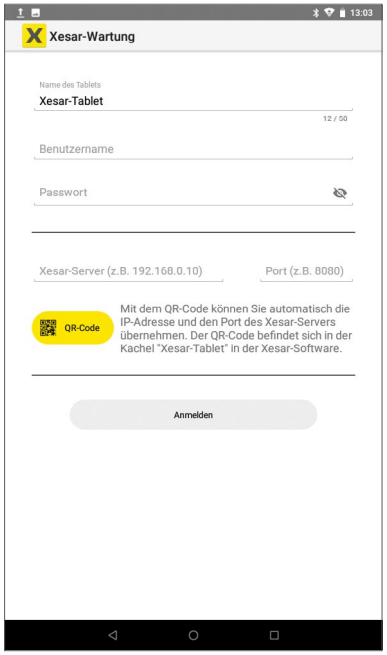
Zum Verbinden des Tablets mit der Anlage müssen in den Feldern „Xesar-Server" und „Port" die IP-Adresse und der Port (Standard 8080) der Anlage eingegeben werden.

Eine einfachere Möglichkeit ist die Server IP-Adresse und die Port-Adresse mittels QR-Code zu übernehmen.

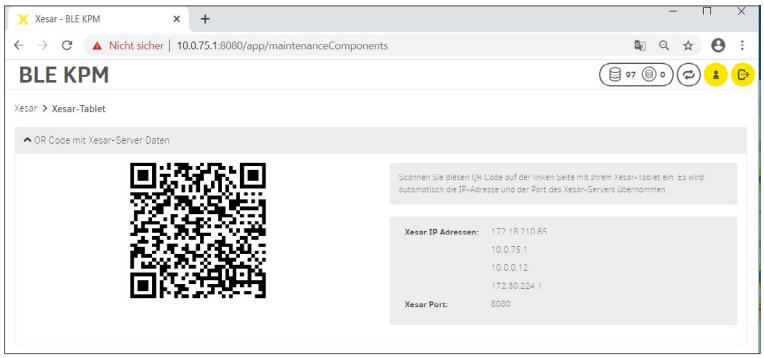
» Klicken Sie auf den Button **QR-Code**
» Nehmen Sie mit der Kamera des Tablets den QR-Code auf der Tablet-Seite der Xesar-Software auf.

Die korrekten Daten werden automatisch in den Login übernommen.

Nach einem Logout und einem neuerlichen Login bleiben bis auf das Passwort des Benutzers alle Einträge erhalten.



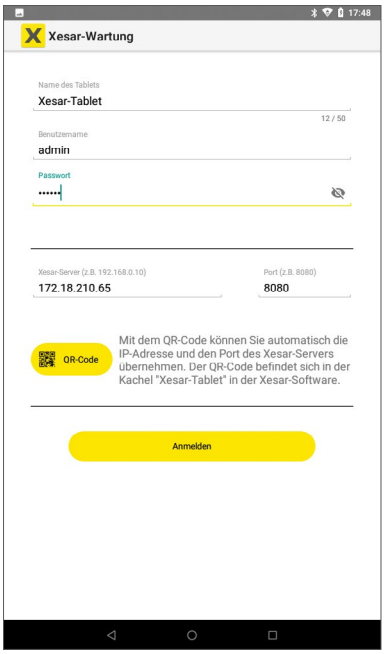
QR-Code mit IP-Adressen und Port-Adressen auf der Xesar-Tablet Dashboard-Seite:



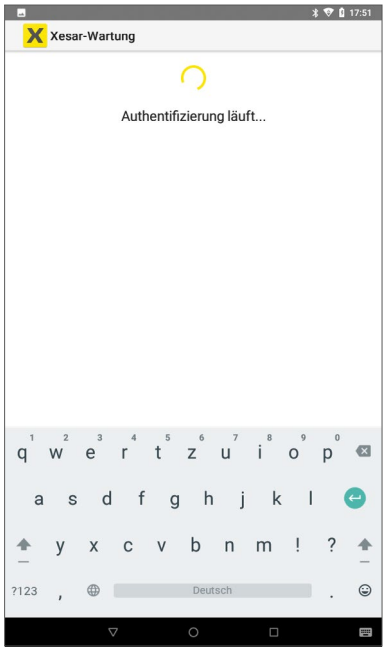
Zur Verwendung des QR-Codes mit der Tablet-Kamera muss am Tablet die Aufnahme von Fotos und Videos zugelassen werden.

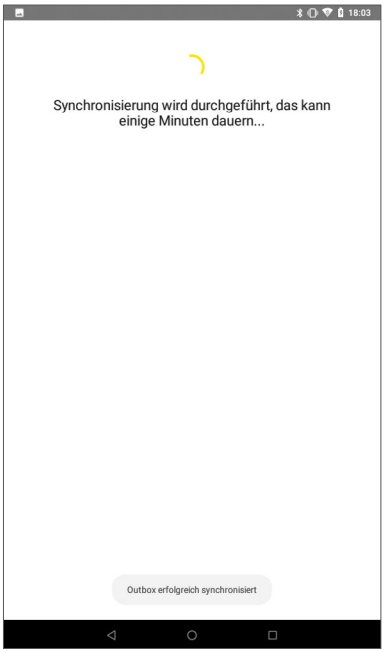
» Drücken Sie den Button **QR-Code** und richten Sie die Kamera des Tablets auf den QR-Code in der Kachel „Xesar-Tablet" auf der Dashboard-Seite. Die IP-Adresse und der Port der Anlage werden automatisch in die entsprechenden Felder übernommen.

» Klicken Sie auf **Anmelden**
Wenn alle Eingabefelder, inklusive Passwort, ausgefüllt wurden, wird der Button „Anmelden" aktiv.



Nach erfolgreicher Authentifizierung des Tablets startet die Synchronisation mit der Anlage. Dabei werden die Wartungsaufgaben auf das Tablet übertragen.
Dieser Vorgang kann je nach Umfang und Datenmenge einige Minuten dauern.





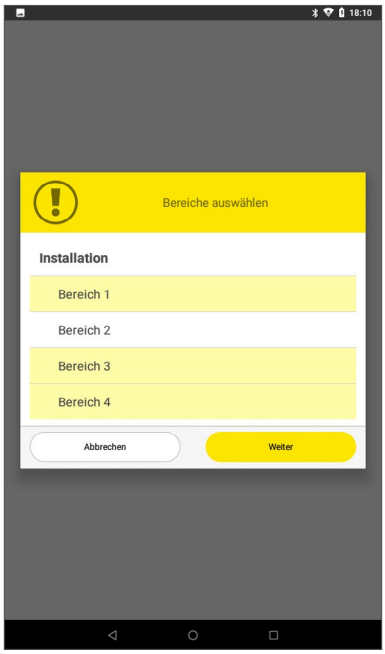
Wenn Sie in der Anlage Einbauorte in Bereiche aufgeteilt haben, erscheint die Auswahlmöglichkeit der Bereiche zur Durchführung der jeweiligen Wartungsaufgaben.

» Es können ein oder mehrere Bereiche ausgewählt werden.

Wenn Sie keine Bereiche in der Anlage eingerichtet haben, werden alle Wartungsaufgaben ohne Bereichsauswahl angezeigt.

Der Bereich „Installation" umfasst alle Bereiche und alle Einbauorte. Bei der Auswahl „Installation" werden alle Wartungsaufgaben der Anlage angezeigt.

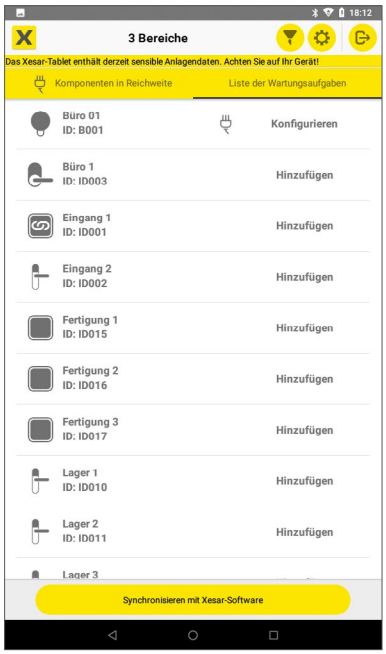
Der Name des ausgewählten Bereichs oder die Anzahl der ausgewählten Bereiche werden in der Kopfzeile angezeigt.



» Bestätigen Sie die Auswahl mit **Weiter**.

20.3 Wartungsaufgaben

Nach erfolgreicher Synchronisation mit der Xesar-Software wird die Liste aller offenen Wartungsaufgaben im Anzeige- und Funktionsfenster angezeigt



» Wischen Sie am Screen nach rechts oder klicken Sie auf die Seitenüberschrift **Komponenten in Reichweite**, um zum Funktionsfenster der „Komponenten in Reichweite" zu wechseln.

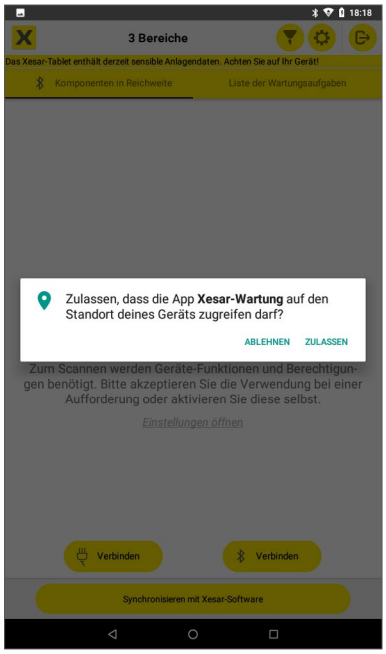
Hier können Sie die offenen Wartungsaufgaben nach dem Verbinden mit den Zutrittskomponenten ausführen.

» Klicken Sie auf den jeweiligen Button **Verbinden**, um das Tablet mit allen Bluetooth-Komponenten Verbinden in Reichweite oder mit der mittels Kabel Verbinden angesteckten Zutrittskomponenten zu verbinden.

20.3.1 Verbinden mit Bluetooth-Komponenten

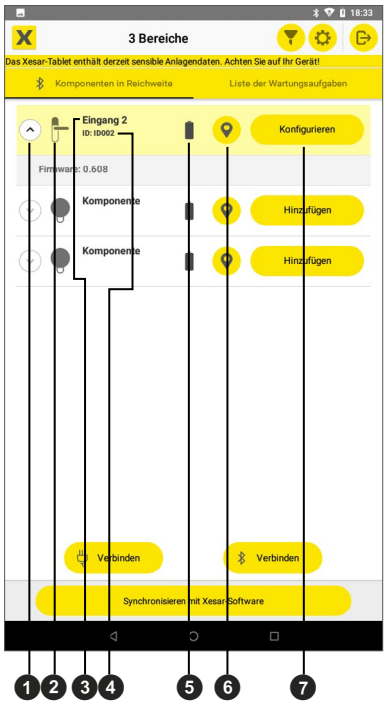
» Drücken Sie den Bluetooth (BLE) **Verbinden**-Button Verbinden, um das Tablet mit allen in Reichweite befindlichen BLE-Komponenten zu verbinden. Beim erstmaligen Drücken des BLE Verbinden-Buttons erfolgt die Standortabfrage, die Sie zulassen müssen.

Die Sende- und Empfangsreichweite zwischen Tablet und BLE-Komponenten ist abhängig von den baulichen Gegebenheiten und beträgt einige Meter.



20.3.2 Ansicht der verbundenen Bluetooth-Komponenten in Reichweite

Hier finden Sie folgende Funktionen und Informationen:



❶ Pfeilbutton
öffnet und schließt das Zusatzfeld

❷ Komponentensymbol
zeigt den Komponententyp des Einbauorts

❸ Name des Einbauorts
wird angezeigt, wenn die Zutrittskomponente in der Anlage eingebaut ist. Ist die Zutrittskomponente im Baustellenmodus, wird „Komponente" angezeigt

❹ ID des Einbauortes
wird angezeigt, wenn die Zutrittskomponente in der Anlage eingebaut ist. Bei Zutrittskomponenten im Baustellenmodus kann diese nicht angezeigt werden.

❺ Batteriesymbol
zeigt den Batteriestatus der Zutrittskomponente an („Batterie voll" oder „Batterie leer"). Wenn an der Zutrittskomponente „Batterie leer" angezeigt wird, müssen die Batterien umgehend gewechselt werden. (Siehe dazu auch Kapitel „Ereignissignalisierung".)

Wenn das Signal „Batterie leer" das erste Mal angezeigt wird, sind für einen Zeitraum von 4 Wochen maximal 1.000 Öffnungen möglich. Die Anzahl der Öffnungen ist abhängig von der Raumtemperatur und kann entsprechend geringer sein.

Wenn kein Batterietausch vorgenommen wird und die Batterien leer sind, kann die Zutrittskomponente nur mit dem optionalen Notstromgerät und einem Zutrittsmedium mit Generalhauptschlüssel-Berechtigung geöffnet werden.

❻ **Identifikationsbutton**
Durch Klicken auf den Identifikationsbutton werden ein optisches und ein akustisches Signal an der jeweiligen Zutrittskomponente ausgelöst. Damit kann die gewünschte Zutrittskomponente eindeutig identifiziert werden.

❼ **Wartungsaufgabebutton**
Durch Klicken auf den Wartungsaufgabebutton wird die entsprechende Wartungsaufgabe gestartet. Sind mehrere BLE-Komponenten mit Wartungsaufgaben mit dem Tablet verbunden, können alle Aufgaben durch Klicken auf den jeweiligen Button aktiviert werden.

Die Wartungsaufgaben werden in der Reihenfolge der Auswahl durchgeführt.

Soll eine Wartungsaufgabe in der Warteschlange nicht durchgeführt werden, kann sie durch Klicken auf das Symbol „x" aus der Vorauswahl entfernt werden. Alle anderen Wartungsaufgaben werden durchgeführt.

Während der Durchführung einer Wartungsaufgabe sind alle Buttons deaktiviert und daher grau.

» Klappen Sie mit dem Pfeilbutton das Zusatzfeld zum Anzeigen weiterer Informationen und Funktionen auf. Hier finden Sie die aktuelle Firmware-Version der Zutrittskomponente und den Button zum Updaten der Firmware, wenn eine neuere Version am Tablet vorhanden ist sowie den Button zum Zurücksetzen der Zutrittskomponente. (Siehe auch Kapitel „Firmware Update“.)

20.3.3 Zutrittskomponente hinzufügen

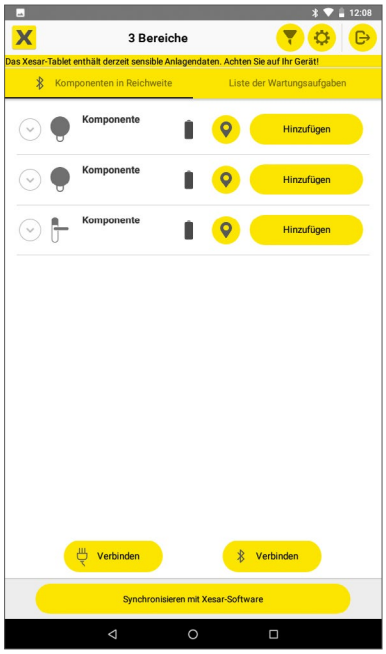
Wenn eine Zutrittskomponente zur Anlage hinzugefügt werden soll, werden die möglichen Einbauorte zum Hinzufügen angezeigt.

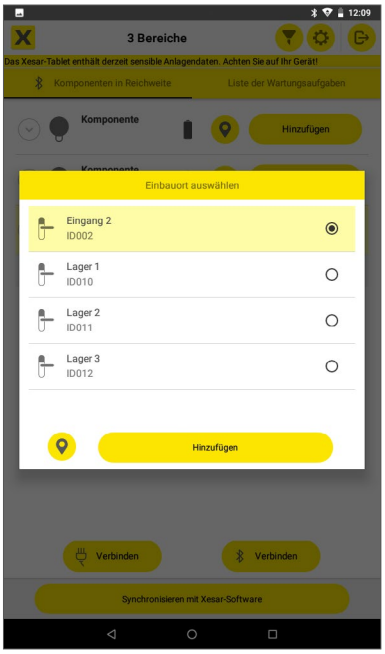
» Wählen Sie den gewünschten Einbauort aus und drücken Sie **Ausführen**.
Zur Identifizierung kann mit dem Identifizierungsbutton die Zutrittskomponente angesteuert werden. Die entsprechende Zutrittskomponente gibt eine akustische und optische Signalisierung ab.

Zum Hinzufügen einer neuen Zutrittskomponente zur Anlage muss der PIN-Code eingegeben werden.

Der vierstellige PIN-Code kann in der Xesar-Software unter „Einstellungen“ frei konfiguriert werden.

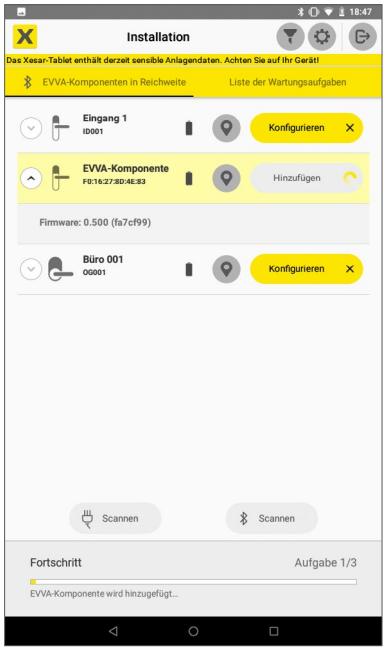
Die PIN-Code-Abfrage kann auch deaktiviert werden.

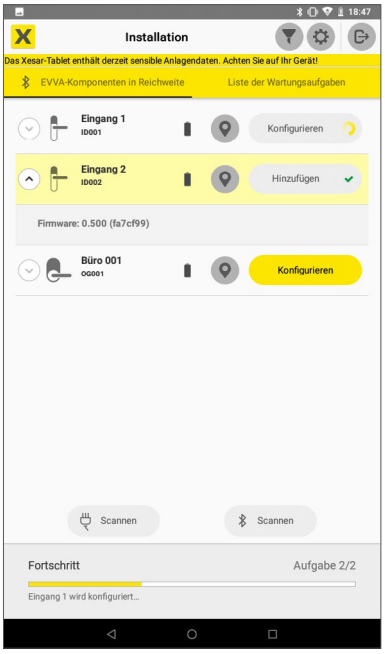




20.3.4 Mehrkomponenten-Konfiguration

Zur schnelleren Durchführung der Wartung wählen Sie alle Wartungsaufgaben der Komponenten in Reichweite aus. Diese Wartungsaufgaben werden entsprechend der Auswahlreihenfolge durchgeführt.
Ausgewählte Wartungsaufgaben können durch nochmaliges Klicken aus der Ablaufreihenfolge entfernt werden. Sie wird nicht durchgeführt und bleibt als „offene Wartungsaufgabe" bestehen.



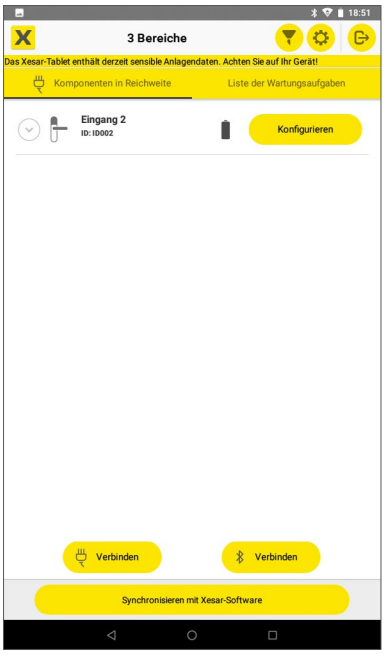


Wenn keine BLE-Komponenten in Reichweite sind, wird nach dem Drücken des BLE Verbinden-Buttons folgendes Bild angezeigt

20.3.5 Verbinden mit einer Kabel-Zutrittskomponente

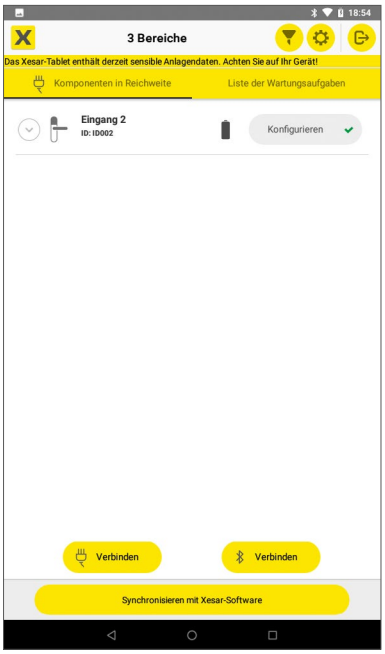
» Verbinden Sie das Tablet und eine Zutrittskomponente mit dem USB-Kabel

» Drücken Sie den Kabel **Verbinden**-Button Verbinden.



» Führen Sie anschließend die Wartungsaufgabe durch.

Die erfolgreiche Durchführung der Wartungsaufgabe wird mit dem grünen Haken-Symbol im Button angezeigt.



» Synchronisieren Sie das Tablet mit der Xesar-Software, nachdem Sie alle Wartungsaufgaben durchgeführt haben. Dadurch werden die neuen Zustände der Zutrittskomponenten in der Xesar-Software bestätigt und die Anzeige der offenen Wartungsaufgaben zurückgesetzt.

Synchronisationsaufgaben der Zutrittskomponenten zum Abholen von Zutrittslogs und zum Setzen der Uhrzeit in den Zutrittskomponenten können jederzeit auch ohne offene Wartungsaufgaben durchgeführt werden.

Deaktivieren Sie im Filter die Funktion „Sync-Aufgaben ausblenden", damit in der Liste der Wartungsaufgaben Zutrittskomponenten zur Synchronisation angezeigt werden.

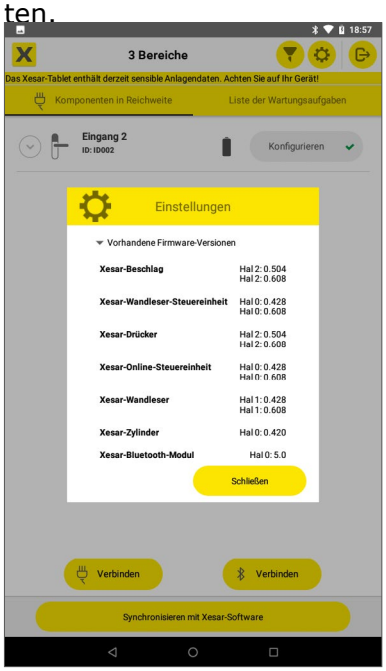
20.4 Einstellungen

Unter Einstellungen können folgende Informationen abgerufen und Einstellungen vorgenommen werden.

- **Version der Xesar-Wartungsapp**
  zeigt die aktuelle Version der Xesar-Wartungsapp an.

- **Ereignisprotokollübertragung**
  Bei aktivierter Checkbox wird das Ereignisprotokoll bei allen Wartungs- und Synchronisationsaufgaben von den Zutrittskomponenten auf das Tablet übertragen. Das kann zu einer längeren Dauer der Wartungsaufgaben führen. Bei deaktivierter Checkbox wird das Ereignisprotokoll nur bei Synchronisationsaufgaben übertragen. Das Ereignisprotokoll enthält alle Zutritte und Abweisungen der Zutrittskomponente und wird mittels Tabletsynchronisation oder über XVN zur Xesar-Software übertragen.

- **Zutrittskomponenten-Firmware**
  zeigt alle auf dem Tablet vorhandenen Firmware-Versionen der Zutrittskomponenten.



- **Firmware-Versionen aktualisieren**
  Drücken Sie auf **Aktualisieren**, um die Firmware-Versionen am Tablet über das Internet vom EVVA-Server zu aktualisieren.

> Zum Aktualisieren der Firmware-Versionen ist eine Internetverbindung des Tablets mittels WLAN notwendig.

- **Letzte Überprüfung**
  Datum der letzten erfolgreichen Prüfung der Firmware-Versionen

20.4.1 Firmware-Update

Firmware-Updates gewährleisten einen sicheren und reibungslosen Betrieb der Anlage. Sie ermöglichen funktionelle Verbesserungen und neue Funktionen der Zutrittskomponenten.

Zutrittskomponenten mit nicht aktueller Firmware werden am Dashboard angezeigt.

Durch Synchronisieren des Tablets mit der Xesar-Software werden die in der Xesar-Software enthaltenen Firmware-Versionen auf das Tablet geladen. Hat eine Zutrittskomponente eine ältere Firmware-Version, kann diese Zutrittskomponente mit einem Firmware-Update aktualisiert werden.

Zum Firmware-Update einer Zutrittskomponente wird eine Wartungsaufgabe erstellt und in der Liste der Wartungsaufgaben angezeigt.

» Verbinden Sie die Zutrittskomponente mit dem Tablet (über Kabel oder drahtlos mittels BLE).

» Führen Sie die Wartungsaufgabe durch Klick auf den Wartungsaufgabe-Button durch.

20.4.2 Firmware-Update im Baustellenmodus

Befindet sich eine Zutrittskomponente im Baustellen,Modus, kann ein Firmware-Update auch dann durchgeführt werden, wenn das Tablet nicht mit einer Anlage verbunden ist.

Halten Sie die Firmware aller Zutrittskomponenten aktuell und führen Sie Firmware-Updates immer durch.

Ist eine neuere Firmware-Version, als die in der Xesar-Software installierten, vorhanden, kann die neue Firmware-Version unter „Einstellungen" über das Tablet mittels Aktualisieren auf das Tablet geladen werden. Dazu muss das Tablet über WLAN mit dem EVVA-Server über das Internet verbunden sein. Diese aktuelle Firmware kann nach Bedarf – wie oben beschrieben – auf die jeweiligen Zutrittskomponenten geladen werden. Es werden dazu keine Wartungsaufgaben erstellt.

» In der Ansicht „Komponenten in Reichweite“ klappen Sie die Detailansicht der jeweiligen Zutrittskomponente auf und führen Sie das Firmware-Update durch.

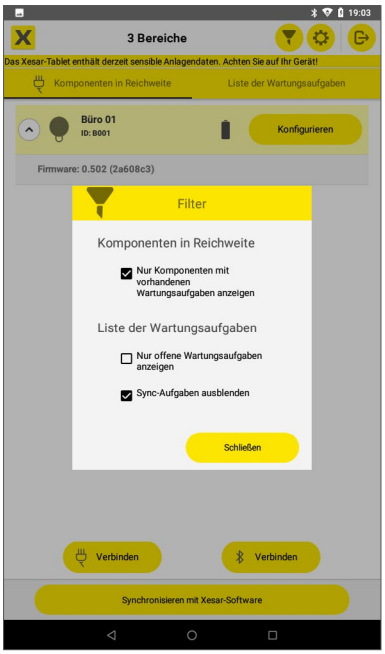
20.5 Filter

Unter den Filteroptionen können Einstellungen zu den Ansichten der Seiten „Komponenten in Reichweite“ und „Liste der Wartungsaufgaben“ vorgenommen werden.

- **Nur Komponenten mit vorhandenen Wartungsaufgaben anzeigen**
  Wenn die Checkbox aktiviert und ein Scan durchgeführt wird, dann werden nur die in Reichweite befindlichen BLE-Komponenten der betreffenden Anlage und Zutrittskomponenten im Baustellenmodus, für die eine Wartungsaufgabe vorhanden ist, angezeigt. Zutrittskomponenten anderer Anlagen, die auch in Reichweite sind, werden nicht angezeigt.
  Sollen alle vorhandenen Zutrittskomponenten in Reichweite angezeigt werden, muss die Checkbox deaktiviert werden.

- **Liste der Wartungsaufgaben**
  „Nur offene Wartungsaufgaben anzeigen“ aktivieren, um nur die noch offene Wartungsaufgaben anzuzeigen. Bereits erledigte Aufgaben werden ausgeblendet.

- **Sync-Aufgaben ausblenden**
  Wenn die Checkbox aktiviert, ist werden in der Liste der Wartungsaufgaben nur Zutrittskomponenten mit Wartungsaufgaben angezeigt und Zutrittskomponenten mit möglichen Synchronisationsaufgaben ausgeblendet.



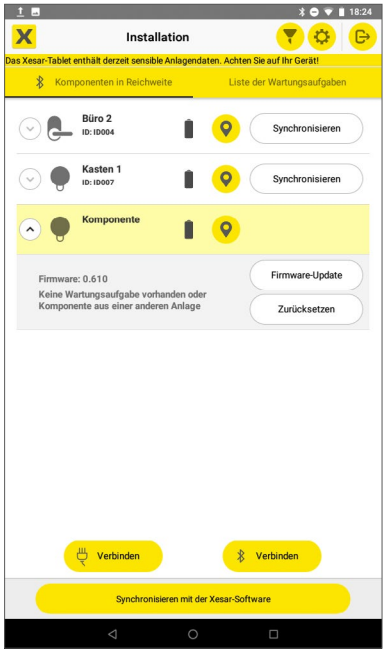
20.6 Eine Zutrittskomponente in den Baustellenmodus zurücksetzen

Wenn eine Zutrittskomponente in der Xesar-Software aus der Anlage entfernt wurde, wird sie nach der Durchführung der entsprechenden Wartungsaufgabe in den Baustellenmodus zurückgesetzt. In diesem Zustand kann Sie an einem anderen Einbauort oder in einer anderen Anlage hinzugefügt werden.

Eine defekte Zutrittskomponente wird in der Xesar-Software mit „defekte Komponente entfernen" aus der Anlage entfernt.

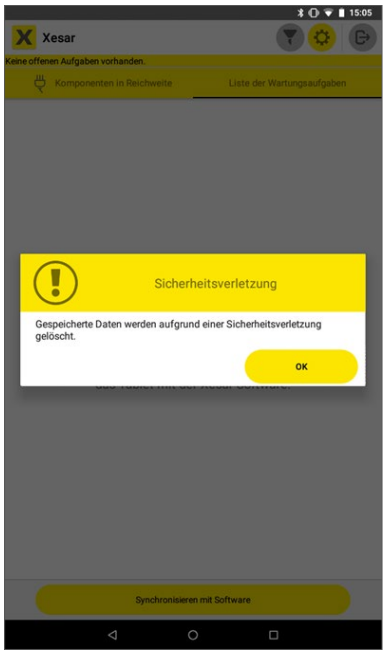
Wird eine Zutrittskomponente irrtümlich als defekt entfernt, kann sie mittels Zurücksetzen am Tablet in den Baustellenmodus gesetzt werden und wieder der Anlage hinzugefügt werden. Wird die Komponente via BLE zurückgesetzt, dann muss der Filter „nur Konfigurationsaufgaben anzeigen" deaktiviert sein, damit die Komponente via BLE-Scan gefunden wird.

Wird eine Zutrittskomponente mit deaktiverter BLE-Sendefunktion in den Baustellenmodus zurückgesetzt, wird die BLE-Funktion aktiviert.



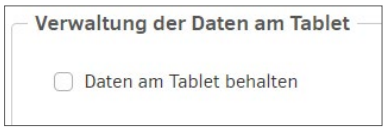
20.7 Weitere Anzeigen

Wenn die Uhrzeit oder die Standortdaten des Tablets im Betriebssystem geändert werden, dann werden aus Sicherheitsgründen die am Tablet gespeicherten Daten gelöscht und folgender Hinweis angezeigt:



20.8 Verwaltung der Daten am Tablet

Sollen Daten auch nach dem Ausschalten des Tablets für eine spätere Durchführung der Wartungsaufgaben gespeichert bleiben, muss das am Dashboard unter „Einstellungen > Verwaltung der Daten am Tablet“ „Daten am Tablet behalten“ ausgewählt werden.



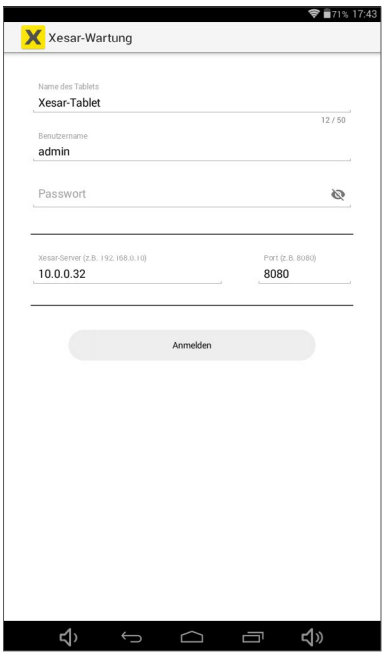
Wenn die Checkbox aktiviert ist, bleiben sicherheitsrelevante Daten auch nach dem Ausschalten des Tablets am Tablet erhalten.
Stellen Sie sicher, dass das Tablet nur durch berechtigte Personen bedient wird.

20.9 Bedienung der Xesar-Wartungsapp auf älteren Tablets

Die Xesar-Wartungsapp kann auch auf einem älteren Tablet, als ARES BLE 4.2. betrieben werden. Aufgrund der fehlenden BLE- und Kamera-Funktionen sind folgende Aktionen jedoch nicht durchführbar:

- Drahtlose Konfiguration von G2.1 BLE-Komponenten
  (Verbinden-Button ist deaktiviert; Verbindung über Kabel ist möglich)

- QR-Code Scan ist nicht möglich.
  (Die IP-Adresse und Port-Nummer zur Tablet-Synchronisation müssen händisch eingegeben werden.)



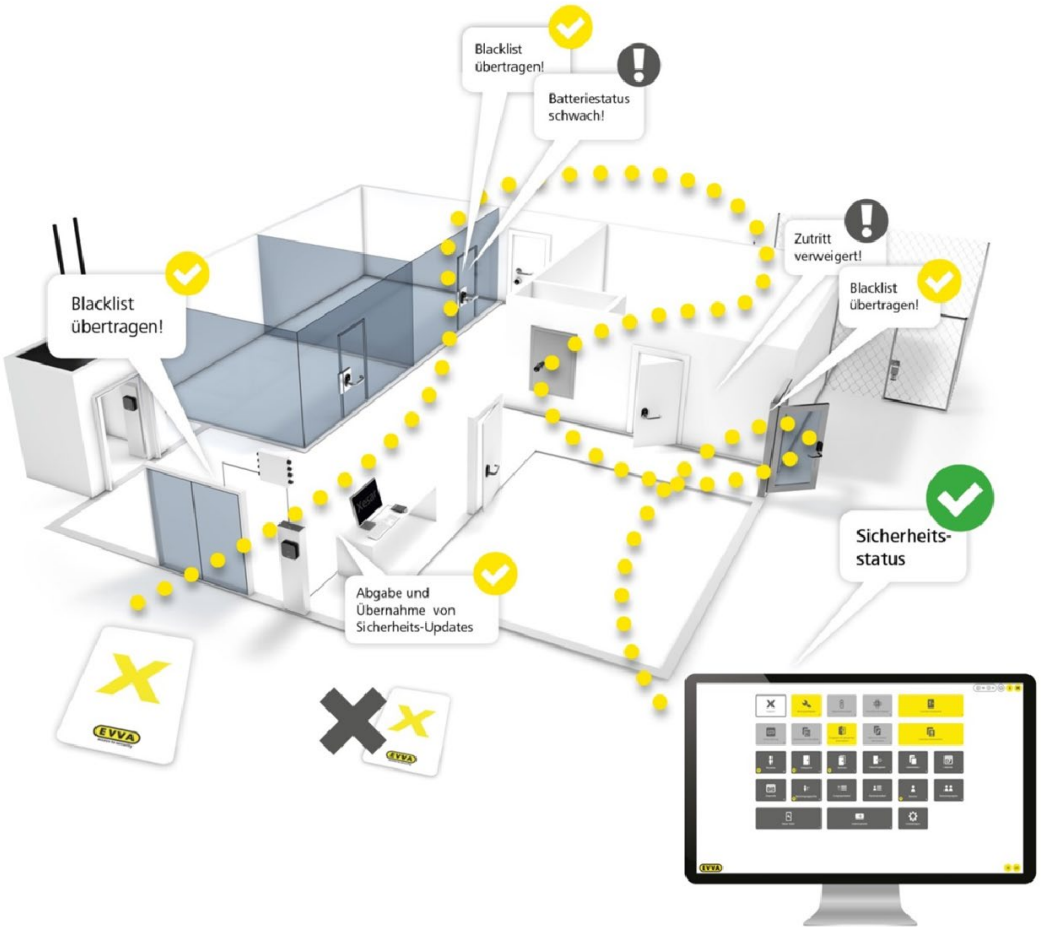
21 Fehlermeldungen Xesar-Tablet

Es kann am Xesar-Tablet aufgrund falscher Handhabung zu unterschiedlichen Fehlermeldungen kommen. Nachfolgend eine Übersicht aller Fehler-Codes sowie einige Hinweise zur Ursache und Fehlerbehebung.

Fehler-Code	Fehlermeldung	Ursache und Fehlerbehebung
XTDE01	Falscher Komponententyp	Es wurde in der Xesar-Software für diesen Einbauort eine andere Zutrittskomponente festgestellt. » Überprüfen Sie die Richtigkeit des Einbauortes und den entsprechenden Xesar-Komponententyp.
XTDE02	USB nicht angeschlossen	Das USB-Kabel ist nicht richtig am Tablet bzw. an der Zutrittskomponente angesteckt oder das USB-Kabel ist defekt. » Überprüfen Sie die Steckverbindungen und den Zustand des Kabels.
XTDE03	Keine Antwort	Es ist ein Fehler am Tablet oder der Zutrittskomponente aufgetreten. » Starten Sie das Tablet nochmals.
XTDE04	Falsche Türe	Zutrittskomponente befindet sich an der falschen Türe. Eventuell wurde eine alte Datenbank wiederhergestellt. » Einbauort bzw. Aktualität der Datenbank prüfen.
XTDE05	Komponente hat keine Batterie	» Legen Sie die vorgegebenen Batterien richtig gepolt in die Zutrittskomponente ein oder » tauschen Sie leere Batterien.
XTDE09	Teilkomponente meldet sich nicht	Der Zylinderknauf wurde nicht korrekt montiert oder der Wandleser nicht korrekt verkabelt. » Überprüfen Sie die Zutrittskomponente auf korrekte Montage und Anschluss.
XTDE10	Version nicht unterstützt	Die Zutrittskomponente hat nicht die richtige Firmware-Version. » Führen Sie ein Firmware-Update im Baustellenmodus mit dem Tablet durch.

Fehler-Code	Fehlermeldung	Ursache und Fehlerbehebung
XTDE11	Fehler USB-Kommunikation	Das USB-Kabel ist nicht richtig am Tablet oder an der Zutrittskomponente angesteckt oder es ist defekt. » Überprüfen Sie die Steckverbindungen und den Zustand des USB-Kabels. » Überprüfen Sie, ob die Zutrittskomponente defekt ist.
XTDE12	Unbekannter Fehler	Unbekannte Ursache. » Versuchen Sie das Tablet auszuloggen und erneut mit der Xesar-Software zu synchronisieren.
XTDE13	Operation temporär fehlgeschlagen	» Versuchen Sie das Tablet auszuloggen und erneut mit der Xesar-Software zu synchronisieren.
XTDE14	Operation fehlgeschlagen	» Versuchen Sie das Tablet auszuloggen und erneut mit der Xesar-Software zu synchronisieren.
XTDE15	Xesar-Tablet nicht synchronisiert	» Synchronisieren Sie das Tablet mit der Xesar-Software.
XTDE16	Batterie anzeigen fehlgeschlagen	» Überprüfen Sie die Batterien der Zutrittskomponenten und tauschen Sie sie bei Bedarf.
XTDE17	----	Das Zurücksetzen einer Xesar-Komponente, die zwangsweise aus der Datenbank entfernt worden ist, schlägt fehl. » Die Zutrittskomponente muss zur Reparatur an EVVA gesendet werden.

22 Xesar Virtuelles Netzwerk (XVN)



An einer zentralen Stelle (Codierstation oder Xesar-Online-Wandleser) werden die Zutrittsmedien mit Update-Informationen (Blacklist) bespielt. Auf dem Weg durch das Gebäude werden diese zu den Türen getragen. Dabei aktualisieren die Zutrittsmedien den Status der Türen und sammeln Informationen der Türen (Batteriestatus, Zutrittsereignisse, Löschungen oder Öffnungen von gesperrten Zutrittsmedien) ein. An der Codierstation werden diese Informationen abgegeben, ausgewertet und der Sicherheitsstatus in der Software aktualisiert.

Bis zu 150 Xesar-Online-Wandleser können in eine Anlage eingebunden werden.

22.1 Übertragung von Zutrittsereignissen über die Zutrittsmedien

Bei jedem zweiten Identifikationsvorgang, z. B. bei der Öffnung einer Zutrittskomponente mittels Zutrittsmedium, werden die letzten Zutrittsereignisse (z. B. Öffnungen, Abweisungen oder Batterie leer) der Zutrittskomponente auf das Zutrittsmedium übertragen.

Wird das Zutrittsmedium an die Codierstation oder den Xesar-Online-Wandleser gehalten, werden die Ereignisse in die Xesar-Software übertragen und das Zutrittsmedium bereinigt.

Für diesen Vorgang ist ein Login der Xesar-Software nicht notwendig, das gestartete Programm ist ausreichend.

22.2 Übertragung von Blacklisteinträgen über die Zutrittsmedien

Ein Blacklisteintrag enthält die Information über ein in der Xesar-Software gesperrtes Zutrittsmedium. Diese Blacklisteinträge werden via Codierstation oder Xesar-Online-Wandleser auf alle Zutrittsmedien geschrieben und so zu allen besuchten Zutrittskomponenten getragen.

Auf einem Zutrittsmedium sind bis zu 10 Blacklisteinträge möglich. Sobald die Zutrittsmedien wieder an der Codierstation oder dem Xesar-Online-Wandleser angehalten werden, erkennt die Xesar-Software, an welche Zutrittskomponenten die Blacklist durch das jeweilige Zutrittsmedium bereits übertragen wurde und visualisiert den entsprechenden Status am Dashboard der Xesar-Software.

Übertragen Sie die Blacklist via Xesar-Tablet, wenn mehr als 10 Identmedien auf einmal verloren gehen oder gestohlen werden.

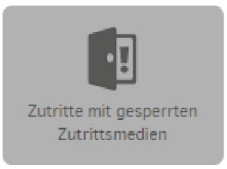
Ein in der Xesar-Software gesperrtes Zutrittsmedium kann ungültig bzw. gelöscht werden, wenn

- das Ablaufdatum überschritten wurde
- die Gültigkeitsdauer überschritten wurde
- das Zutrittsmedium an die Codierstation oder den Xesar-Online-Wandleser gehalten wurde
- das Zutrittsmedium versucht, eine Zutrittskomponente zu öffnen, bei der die Blacklist aktuell ist.

22.3 Übertragung der Information „Zutritte mit gesperrten Zutrittsmedien“

So lange ein in der Xesar-Software gesperrtes Zutrittsmedium noch gültig ist, kann dieses die jeweiligen Zutrittskomponenten auch öffnen. Diese sicherheitskritischen Informationen werden durch andere Zutrittsmedien in der Anlage gesammelt und via Codierstation oder Xesar-Online-Wandleser an die Xesar-Software übermittelt.

Am Dashboard wird das signalisiert. Die Farbe der Kachel **Zutritte mit gesperrten Zutrittsmedien** ist gelb, wenn Öffnungen mit bereits gesperrten Zutrittsmedien stattgefunden haben.



22.4 Übertragung der Information „Zutrittsmedium von Zutrittskomponente gelöscht“

Bei dem Versuch, mit einem in der Xesar-Software gesperrten Zutrittsmedium, eine-Zutrittskomponente mit aktueller Blacklist zu öffnen, wird das Zutrittsmedium von der Zutrittskomponente gelöscht.

Anschließend kann dieses Zutrittsmedium keine Zutrittskomponente ohne aktuelle Blacklist öffnen. Dieses Zutrittsmedium hat somit seine Gültigkeit verloren.

Die Informationen von einem gesperrten, gelöschten Zutrittsmedium werden von anderen Zutrittsmedien via virtuellem Netzwerk zurück zur Xesar-Software übertragen. Dazu müssen die Zutrittsmedien an eine Codierstation oder einen Xesar-Online-Wandleser gehalten werden.

Die Xesar-Software-Benutzer bekommen so automatisch die Information, dass die Anlage wieder sicher ist, obwohl die Blacklist möglicherweise noch nicht bei allen Zutrittskomponenten aktualisiert wurde.

Beachten Sie die Hinweise auf eventuelle Wartungsaufgaben im Dashboard und halten Sie ihre Zutrittskomponenten auf dem neuesten Stand.

22.5 Übertragung des Batteriestatus über die Zutrittsmedien

Über die im Umlauf befindlichen Zutrittsmedien werden via virtuelles Netzwerk auch Batterieinformationen zur Xesar-Software transportiert. Der Anlagenadministrator weiß somit rechtzeitig, wann welche Batterien zu tauschen sind.

Der Anlagenadministrator hat indirekt die Möglichkeit, die Update-Zyklen über die Gültigkeitsdauer der Zutrittsmedien zu beeinflussen. Die Gültigkeitsdauer wird bei jedem Anhalten eines Zutrittsmediums an der Codierstation oder dem Xesar-Online-Wandleser automatisch um den eingestellten Wert verlängert.

Wird z. B. die Gültigkeitsdauer auf 3 Tage eingestellt, muss jede Person mit Zutrittsmedium innerhalb dieser Zeit an der Codierstation oder dem Xesar-Online-Wandleser eine Aktualisierung durchführen, um die Gültigkeit zu verlängern. So bekommt der Anlagenadministrator spätestens nach 3 Tagen die entsprechenden Informationen (z. B. Ereignisse oder Blacklistübertragungen) via der im Umlauf befindlichen Zutrittsmedien. Wird die Gültigkeit auf 30 Tage eingestellt, dauert es dementsprechend länger, bis die Informationen zur Xesar-Software zurück gelangen.

Halten Sie die Gültigkeitsdauer bei Verwendung des virtuellen Netzwerks möglichst kurz, am besten unter 15 Tage.

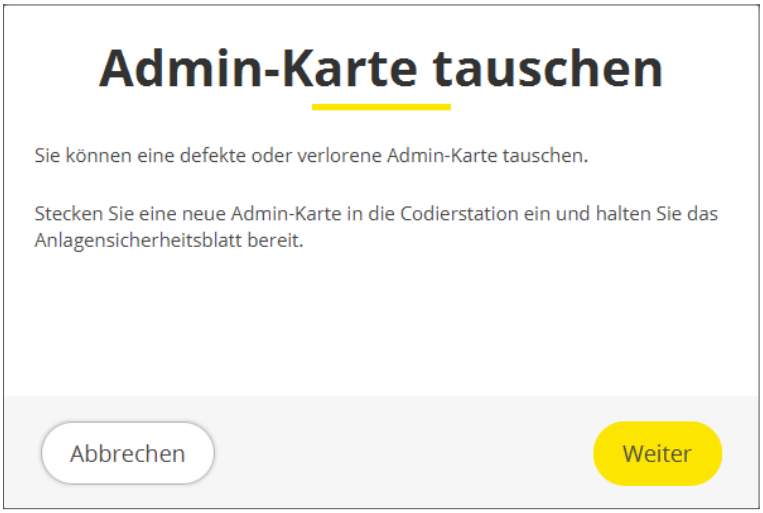
23 Admin-Karte tauschen

23.1 Admin-Karte tauschen bei Xesar-Anlagen auf PC

Siehe auch Kapitel „Startseite Installation-Manager > Konfiguration der Anlage".

Bei Defekt oder Verlust der Admin-Karte der Anlage kann sie gegen eine neue Admin-Karte getauscht werden.

» Klicken Sie dazu in der Konfigurationsseite auf **Admin-Karte tauschen** und folgen Sie den Anweisungen.



23.2 Admin-Karte tauschen bei Xesar-Anlagen auf Server

Ist die Admin-Karte defekt oder verloren gegangen, kann sie wie folgt ausgetauscht werden:

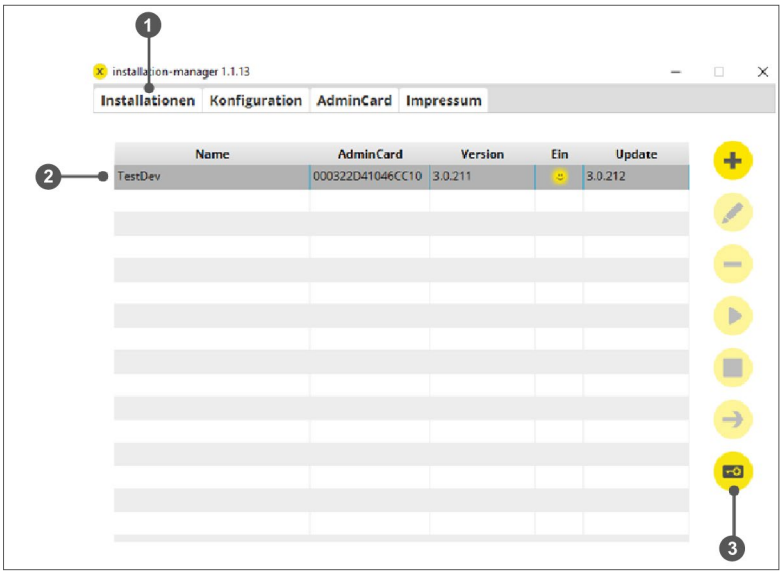
» Stecken Sie eine neue Admin-Karte in die Codierstation.

» Öffnen Sie im Installation-Manager den Tab **Admin-Karte** und laden Sie die neue Admin-Karte.

» Speichern Sie die Einstellung und wechseln Sie zum Tab **Installationen** ❶.

» Wählen Sie die gewünschte Anlage ❷ aus und

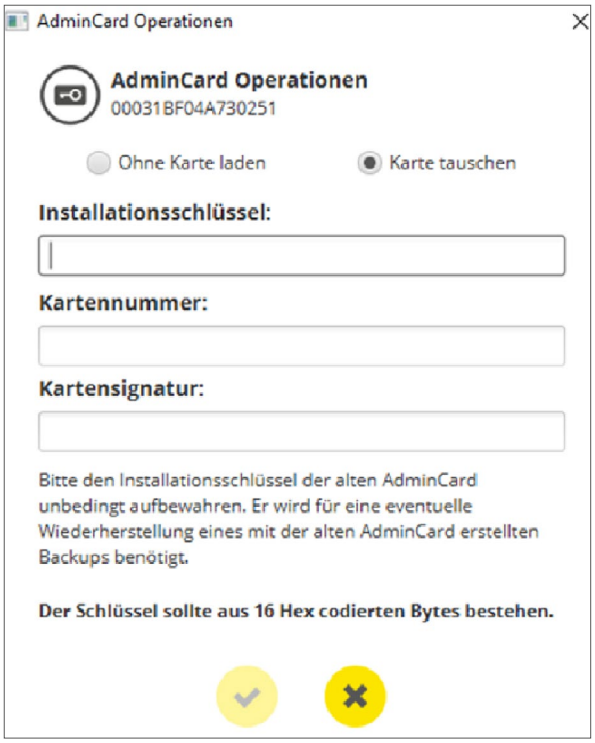
» klicken Sie auf das Smybol **Schlüssel** ❸.

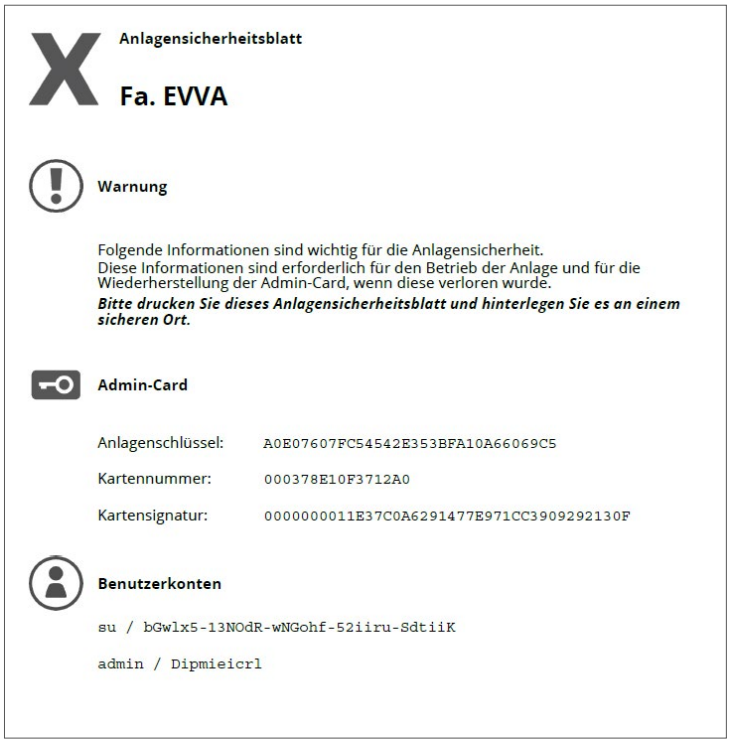


» Wählen Sie im Fenster „AdminCard-Operationen" die Funktion **Karte tauschen**.

» Geben Sie den Installationsschlüssel, die Kartennummer und die Kartensignatur ein.

Diese Daten finden Sie auf dem Anlagensicherheitsblatt, das Sie bei der ersten Installation ausgedruckt haben.





Nach Bestätigung wird ein neues Anlagensicherheitsblatt generiert.

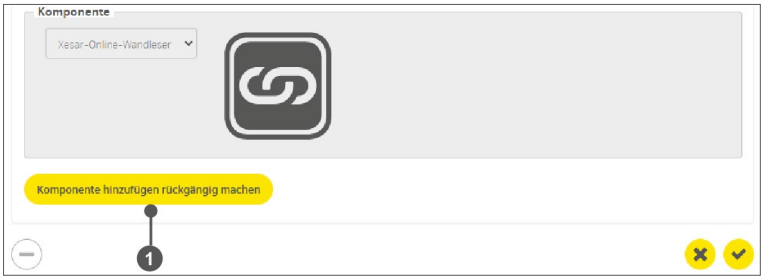
» Drucken Sie das Anlagensicherheitsblatt aus und bewahren Sie es gut auf.

Erstellen Sie nach dem Tausch der Admin-Karte unbedingt ein manuelles Backup im Installation-Manager, damit ein Restore bei Bedarf zur neuen Admin-Karte passt.

23.3 Komponente hinzufügen rückgängig machen

Falls Sie die falsche Komponente beim Einbauort hinzugefügt haben, können Sie die Komponente wieder entfernen.

» Klicken Sie auf den Button **Komponente hinzufügen rückgängig machen ❶**.



Darüber hinaus müssen Sie den Einbauort nicht neu erstellen, sondern können einfach eine neue Zutrittskomponente auswählen.

Diese Vorgangsweise funktioniert nur vor dem Hinzufügen der Zutrittskomponente und falls erforderlich nach dem Rücksetzen in den Baustellenmodus.

23.4 Komponente ausbauen (Rücksetzen in den Baustellenmodus)

Wenn eine Zutrittskomponente wieder ausgebaut und noch weiterverwendet werden soll, wählen Sie **Komponente entfernen**.

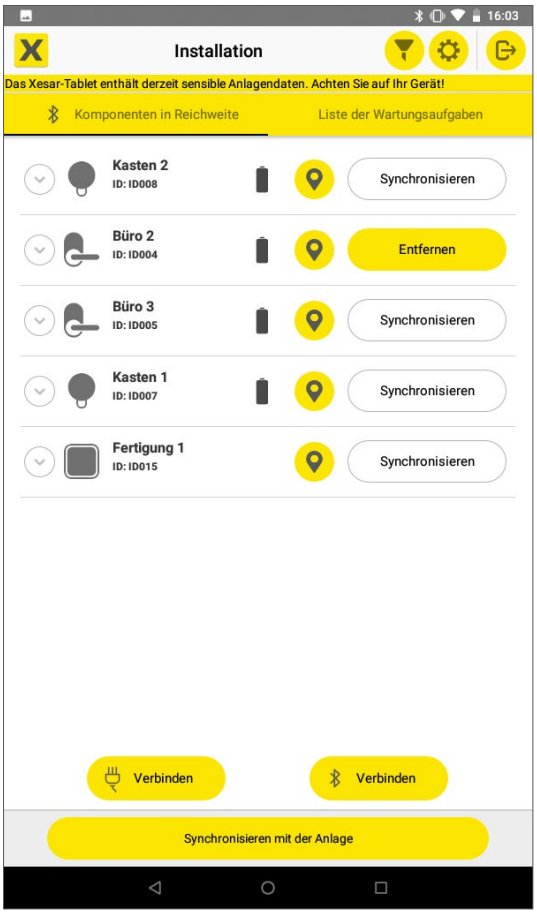
Wenn Sie die Komponente erneut in der Anlage einbauen wollen, klicken Sie NICHT auf **Defekte Komponente entfernen**.

Wenn Sie in der Xesar-Software die Zutrittskomponente entfernt haben, entsteht automatisch eine Wartungsaufgabe. Es muss die Zutrittskomponente mit dem Xesar-Tablet ausgebaut werden.

» Verbinden Sie die Zutrittskomponente mit dem Xesar-Tablet und

» wählen Sie die Zutrittskomponente am Xesar-Tablet aus.

» Führen sie die Wartungsaufgabe **Entfernen** aus.



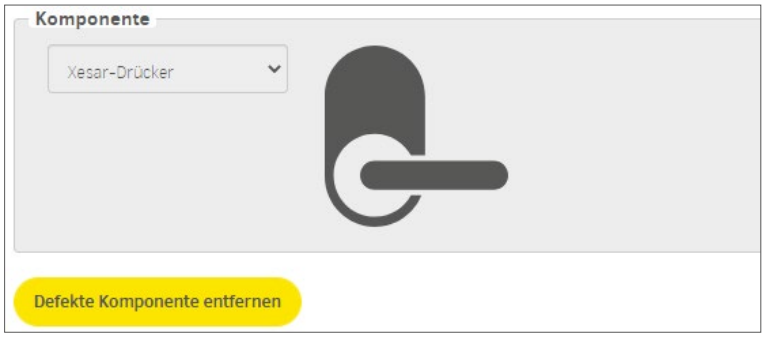
23.5 Komponente erzwungen ausbauen (Komponente defekt)

Wenn eine Zutrittskomponente defekt ist, gehen Sie wie folgt vor:

» Wählen Sie im Menü Einbauorte den entsprechenden Einbauort.

» Wählen Sie in der Liste die zu entfernende Zutrittskomponente und

» klicken Sie auf **Defekte Komponente entfernen**.



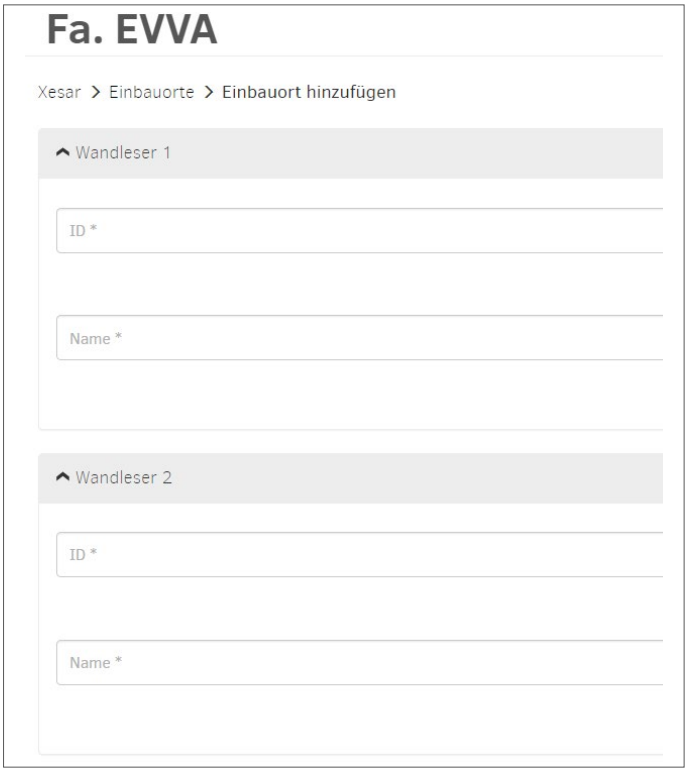
24 Offline Steuereinheit mit 2 Wandleser

24.1 Wandleser hinzufügen

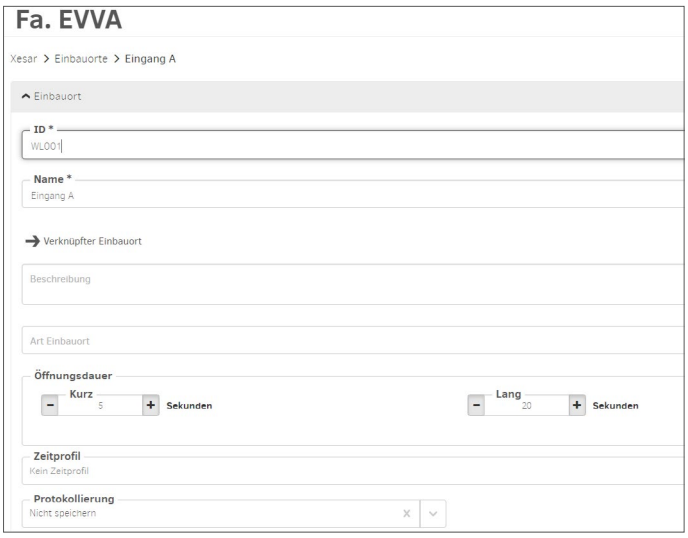
Sie wollen 2 Einbauorte (Türen) mit je einem Wandleser und einer gemeinsamen Steuereinheit ausstatten.

» Wählen Sie bei „Einbauort hinzufügen" die Komponente „Xesar-Steuereinheit mit 2 Wandleser" aus, um 2 Wandleser mit einer Offline-Steuereinheit hinzuzufügen.

» Tragen Sie die IDs und die Namen in die Felder der beiden gewünschten Einbauorte ein.

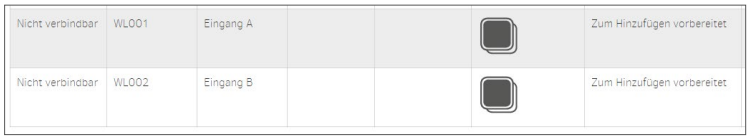


» Konfigurieren Sie die beiden Einbauorte, indem Sie durch Klicken auf → Verknüpfter Einbauort zwischen den beiden Einbauorten wechseln.



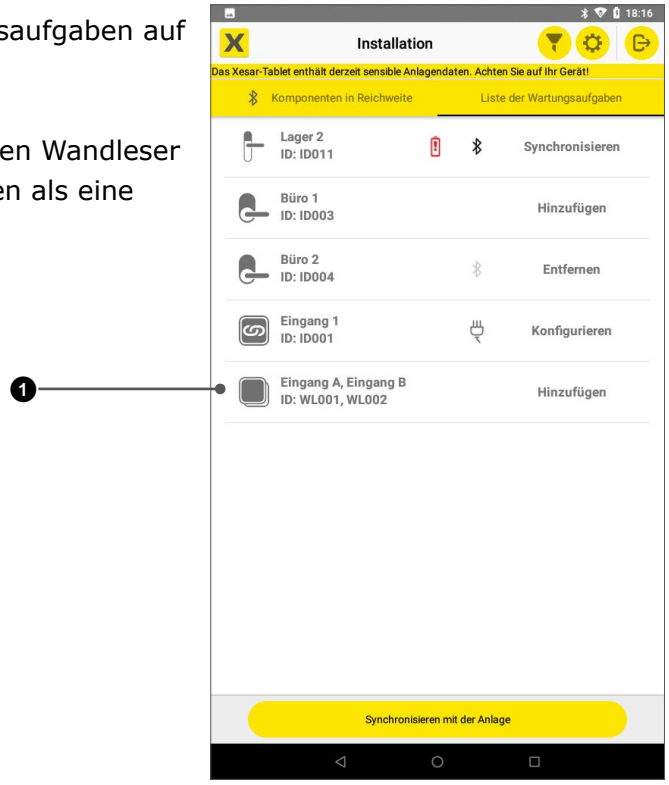
Nach der Bestätigung der Eingaben sind beide Wandleser-Einbauorte in der Anlage angelegt und Wartungsaufgaben für das Hinzufügen erstellt.

In der Liste der Einbauorte sind die beiden verknüpften Wandleser mit dem Zustand „Zum Hinzufügen vorbereitet“ beschrieben.

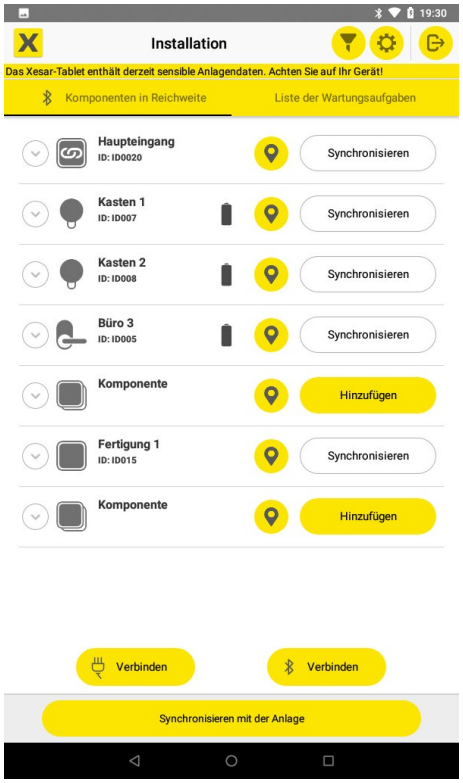


» Synchronisieren Sie die Wartungsaufgaben auf Ihr Xesar-Tablet.

Am Xesar-Tablet werden die beiden Wandleser in der Liste der Wartungsaufgaben als eine Wartungsaufgabe ❶ angeführt.

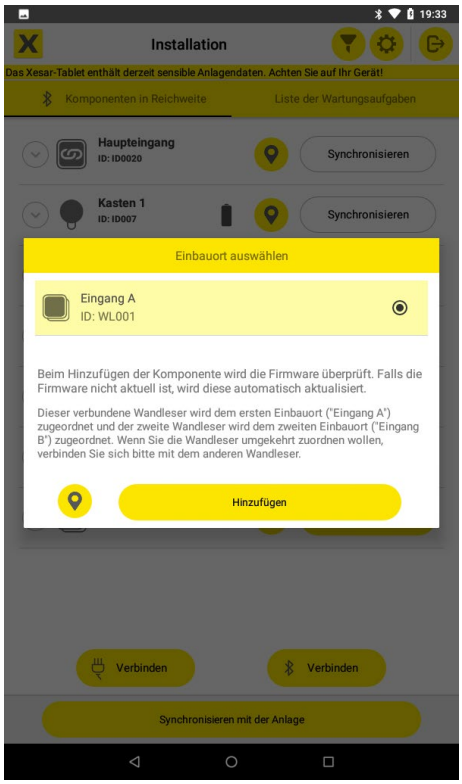


» Verbinden Sie Ihr Xesar-Tablet mit den Wandlesern und führen Sie eine der beiden Wartungsaufgaben durch.



» Vor dem Hinzufügen des ausgewählten Wandlesers überprüfen Sie die richtige Zuordnung zum Einbauort mit der Identifizierungsfunktion.

Es erscheint folgende Mitteilung am Tablet:



» Ist die Zuordnung nicht korrekt, wählen Sie den anderen Wandleser.

Der zweite Wandleser wird automatisch zum zweiten Einbauort hinzugefügt.

Beim Hinzufügen wird die Aktualität der Firmware überprüft und bei Bedarf aktualisiert.

24.2 CU – 2 Wandleser Wartungsaufgaben durchführen

Sie müssen die Wartungsaufgaben für die jeweiligen Wandleser direkt an den entsprechenden Wandlesern durchführen.

» Verbinden Sie das Xesar-Tablet mit dem jeweiligen Wandleser und

» führen Sie die Wartungsaufgaben durch.

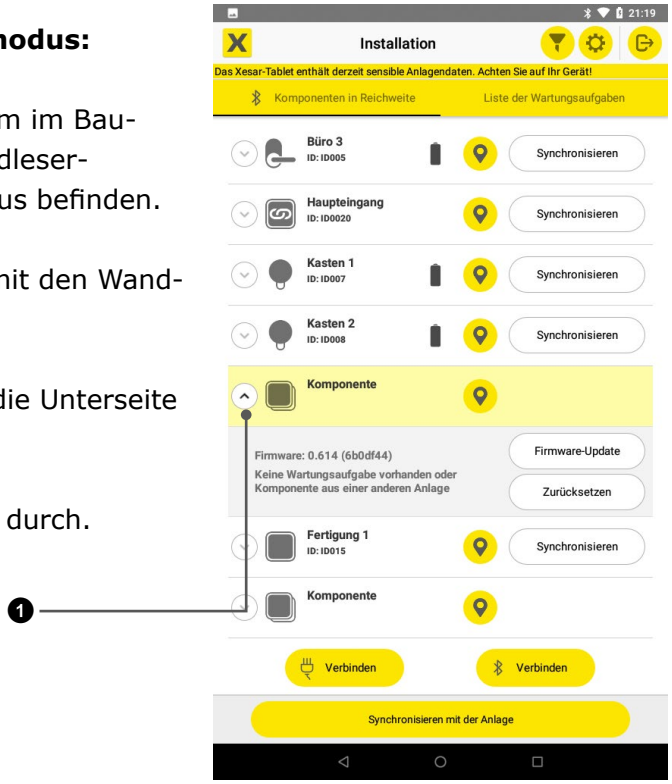
24.3 CU – 2 Wandleser Firmware-Update

Für eine fehlerfreie Funktion der Wandleser müssen alle Teilkomponenten (Wandleser und Steuergerät) die gleiche Firmwareversion aufweisen.

Ein Firmware-Update für die Wandleser und die Steuereinheit führen Sie wie folgt durch:

Firmware Update im Baustellenmodus:

- Überprüfen Sie mit einem Medium im Baustellenmodus, dass sich die Wandleser-Komponenten im Baustellenmodus befinden.
- Verbinden Sie das Xesar-Tablet mit den Wandlesern.
- Klicken Sie auf den Pfeil ❶, um die Unterseite zu öffnen und
- führen Sie das Firmware-Update durch.



Werden im Zuge eines Wandleser- oder Steuergerätetauschs Komponenten mit unterschiedlichen Firmwareversionen kombiniert, müssen die Teilkomponenten im Baustellenmodus auf die aktuelle Firmwareversion aktualisiert werden.

24.4 Wandleserkomponenten aus der Anlage entfernen

» Wählen Sie am Einbauort in der Software **Komponente entfernen** und bestätigen Sie die Auswahl.

» Synchronisieren Sie das Xesar-Tablet mit der Software.

» Verbinden Sie das Xesar-Tablet mit den Wandlesern und führen Sie die Wartungsaufgabe **Entfernen** bei einem Wandleser aus.
Der zweite Wandleser wird automatisch ebenfalls entfernt.

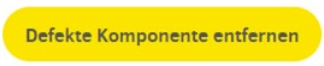
Nach dem Ausbau befinden sich die Komponenten im Baustellemodus.

Sie können nun bei Bedarf ein Firmware-Update durchführen, die Komponenten in eine andere oder dieselbe Xesar-Anlage wieder einbauen.

Wenn eine oder mehrere Komponenten defekt sind:

» Wählen Sie am Einbauort in der Software **Komponente entfernen**

» Wählen Sie anschließend **Defekte Komponente entfernen** aus.



Die als defekt entfernte Komponente muss ersetzt werden.

Wenn Sie irrtümlich eine funktionierende Komponente mit **Defekte Komponente entfernen** aus der Anlage entfernt haben, müssen Sie das Xesar-Tablet mit der Software synchronisieren. Anschließend verbinden Sie das Xesar-Tablet mit der irrtümlich entfernten Komponente und setzen mit Klick auf **Zurücksetzen** diese wieder in den Baustellenmodus zurück. Die zurückgesetzte Komponente kann wieder in der Anlage hinzugefügt werden.

25 Xesar-Online-Wandleser

Der Xesar-Online-Wandleser liest Informationen der Zutrittsmedien, die mit dem XVN (Xesar Virtuelles Netzwerk) gesammelt wurden, aus und liefert sie der Xesar-Software zur weiteren Verarbeitung. Diese Daten sind z. B. Zutrittsereignisse, Abweisungen oder Batteriezustände der Zutrittskomponenten. Gleichzeitig wird die aktuelle Blacklist auf die Zutrittsmedien geschrieben, die Gültigkeitsdauer der Zutrittsmedien verlängert oder Zutrittsmedien-15 durchgeführt. Weiters dient der Xesar-Online-Wandleser als Steuerung für elektrisch angetriebene Zutrittskomponenten, wie Motorschlösser und -zylinder sowie automatische Torantriebe. In Verbindung mit einem Türkontakt kann der Schließzustand der Türe überwacht und angezeigt werden.

Der Xesar-Online-Wandleser bietet folgende Funktionen:

- Update von Zutrittsmedien (Berechtigungsänderungen, Gültigkeitsdauer, Blacklist).
- Zutrittsereignisse: Protokolleinträge in Echtzeit.
- Konfigurationsänderungen des Xesar-Online-Wandlesers in Echtzeit.
- Funktion zur Identifizierung des Xesar-Online-Wandlesers: der gesuchte Xesar-Online-Wandleser gibt wiederholend optisches und akustisches Signal, bis die Funktion wieder deaktiviert wird.
- Office-Mode auslösen und beenden: Start und Ende des Manual-Office-Mode wird protokolliert.
- Zeit setzen: manuelles Zeitsynchronisieren mit dem Xesar-Online-Wandleser, z. B. nach Stromausfall = Offline (wird protokolliert).
- Fernöffnung durchführen: Auf Knopfdruck wird eine protokollierte Fernöffnung durchgeführt.
- Normale Freigabe: Standard-Freigabedauer wird protokolliert.
- Verlängerte Freigabe: Verlängerte Freigabedauer, z. B. für eingeschränkte Personen, wird protokolliert.
- Türaustrittstaster: zum Öffnen von Automatiktüren oder Vereinzelung.
  Jede Betätigung des Türaustrittstasters wird im Ereignisprotokoll protokolliert.
- Türzustandsüberwachung: Abfrage des Zustandes (offen oder geschlossen) des Türkontaktes.
  Bei Serienschaltung Türkontakt mit einem Riegelkontakt kann der Türzustand **geschlossen** und **verriegelt** überwacht werden.

Die verschiedenen Funktionen werden im Ereignis- und im Systemprotokoll protokolliert.

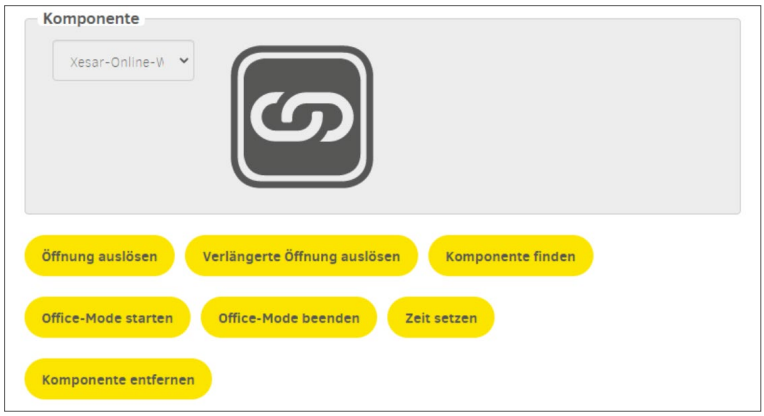
25.1 Xesar-Online-Wandleser hinzufügen

» Fügen Sie zu Ihrer Anlage einen neuen Einbauort hinzu und wählen Sie im Feld „Komponente" den Xesar-Online-Wandleser aus.
» Klicken Sie auf **Weiter**.

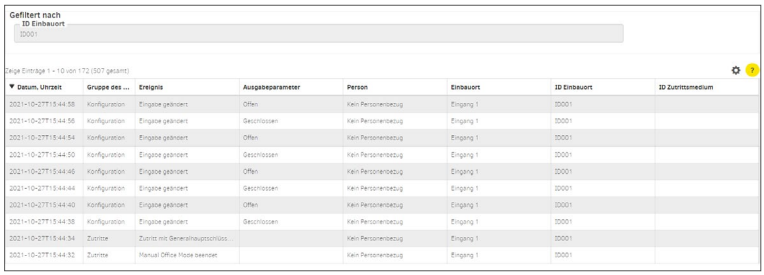
» Geben Sie die entsprechenden Daten ein und
» wählen Sie die gewünschten Einstellungen.

- Zutritte erlauben:
  - Aktiviert funktioniert der Xesar-Online-Wandleser als Medienupdater und als Zutrittskomponente.
  - Deaktiviert funktioniert der Xesar-Online-Wandleser als Medienupdater.
- Upgrade eines Zutrittsmediums erlauben:
  - Aktiviert ist ein Upgrade von Zutrittsmedien möglich. Dies kann auf Grund von Änderungen am Mediendatenformat notwendig sein.

Aus Sicherheitsgründen ist diese Funktion werkseitig deaktiviert und sollte nur bei Bedarf aktiviert werden.



Ereignisprotokoll Türzustandsüberwachung:



Die verschiedenen Funktionen werden im Ereignis- und im Systemprotokoll protokolliert.

2021-10-27T15:44:34	Zutritte	Zutritt mit Generalhauptschlüssel-Medium
2021-10-27T15:44:32	Zutritte	Manual Office Mode beendet
2021-10-27T15:40:30	Zutritte	Manual Office Mode aus Entfernung gestartet
2021-10-27T15:40:24	Zutritte	Manual Office Mode aus Entfernung beendet
2021-10-27T15:40:16	Zutritte	Manual Office Mode gestartet
2021-10-27T15:40:14	Zutritte	Zutritt mit Generalhauptschlüssel-Medium

26 Inbetriebnahme des Xesar-Online Wandleser Netzwerkadapters EXPERT EX9132CST

Überprüfen Sie, dass Sie das passende Modell zur Inbetriebnahmeanleitung in Verwendung haben, bevor Sie den Netzwerkadapter konfigurieren.

Weitere Netzwerkadapter-Inbetriebnahmeanleitungen:

› **https://www.evva.com/at-de/service/downloads/**

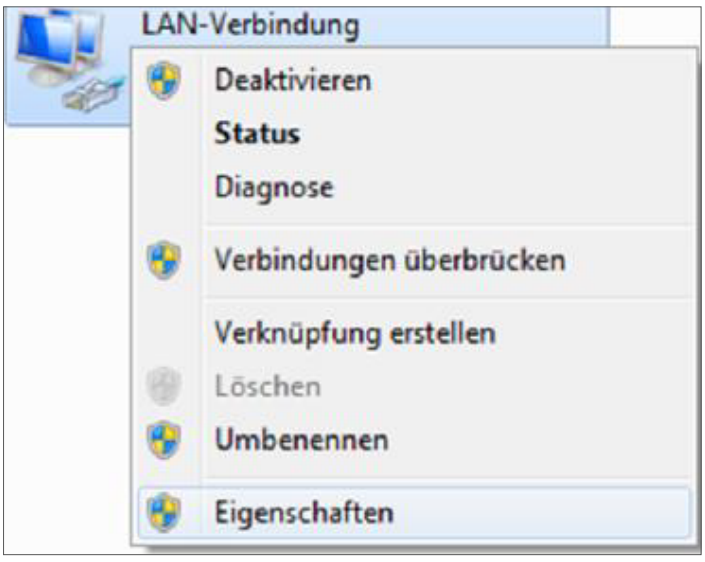
Bei Fragen oder für weitere Informationen wenden Sie sich bitte an an das technische Büro von EVVA.

26.1 PC-Konfiguration

Für die Konfiguration des Xesar-Netzwerkadapters benutzen Sie einen Computer Ihrer Wahl. Das kann auch der PC sein, auf dem die Xesar-Software betrieben wird.

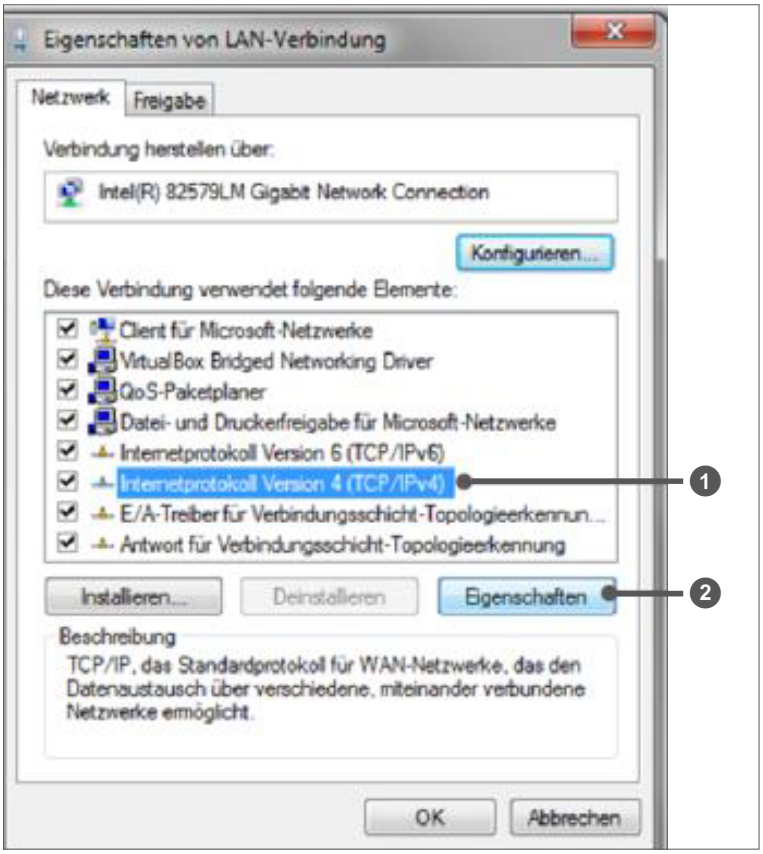
Konfigurieren Sie vorab die Einstellungen Ihres PC-Netzwerkadapters, bevor Sie mit der Inbetriebnahme des Xesar-Netzwerkadapters beginnen. Diese finden Sie z. B. bei Windows 7 oder Windows 10 in Netzwerk- und Freigabecenter > Adaptereinstellungen ändern.

» Öffnen Sie das Eigenschaften-Fenster (Rechtsklick auf die LAN-Verbindung).



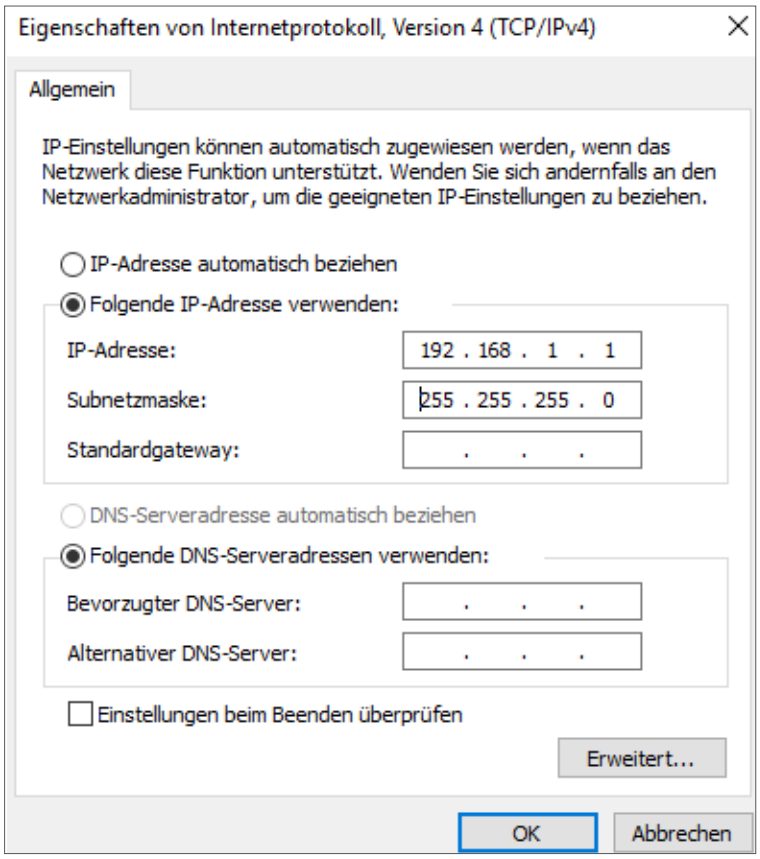
Beachten Sie, dass zusätzlich aktive Netzwerkverbindungen (z. B. WLAN) die Kommunikation mit dem Xesar-Netzwerkadapter stören können. Schalten Sie diese gegebenenfalls ab.

» Wählen Sie im Fenster das Internetprotokoll Version 4 (TCP/IPv4) ❶ und klicken Sie auf Eigenschaften ❷.



» Konfigurieren Sie die IP-Adresse und die Subnetzmaske des PCs 1, mit dem Sie die Konfiguration des Ethernet Adapters vornehmen. Verwenden Sie dafür die folgenden Adressen:

IP-Adresse: 192.168.1.xxx (1-254)
Subnetzmaske: 255.255.255.0
DNS-Server: -



Um einen IP-Adressenkonflikt zu vermeiden, achten Sie darauf, dass Sie **NICHT** die voreingestellte IP-Adresse des Xesar-Netzwerk-adapters (**192.168.1.100**) verwenden.
(Bei IP-Adressenkonflikt kann keine Verbindung aufgebaut werden.)

Wenn Sie Schwierigkeiten beim Einrichten der Netzwerkeinstellungen haben, wenden Sie sich bitte an Ihren IT-Systemadministrator.

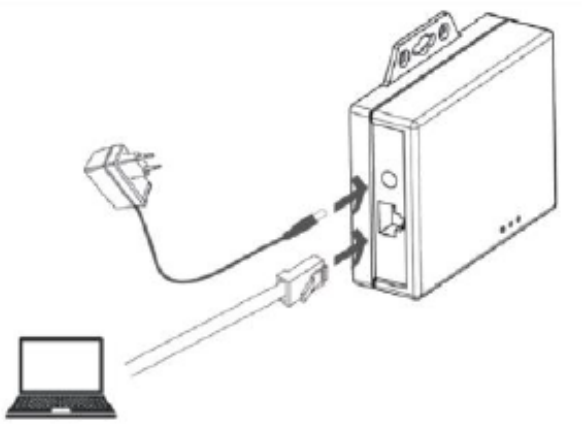
26.2 Inbetriebnahme eines Xesar-Netzwerkadapters

» Verbinden Sie das Netzgerät mit dem Xesar-Netzwerkadapter.

Sie erkennen an der grünen blinkenden Status-LED, ob der Xesar-Netzwerkadapter mit Strom versorgt wird.

» Verbinden Sie den Xesar-Netzwerkadapter mit dem Konfigurations-PC.

Verwenden Sie dazu ein RJ45 LAN-Kabel und achten Sie auf das akustische Klicken, wenn das Kabel einrastet.



» Öffnen Sie den Internet-Browser auf Ihrem Rechner.

» Geben Sie in der Adressleiste des Browsers die Standard-Adresse des Xesar-Netzwerkadapters ein – diese finden Sie auf der Unterseite des Gerätes, sie ist standardmäßig auf **192.168.1.100** gesetzt.

Wenn Sie die Konfigurationsseite nicht öffnen können, kontrollieren Sie die Firewall-Einstellung Ihres PCs, die IP-Einstellungen und die korrekte Verkabelung des Xesar-Netzwerkadapters.

Sie gelangen zur System-Seite des Xesar-Netzwerkadapters.

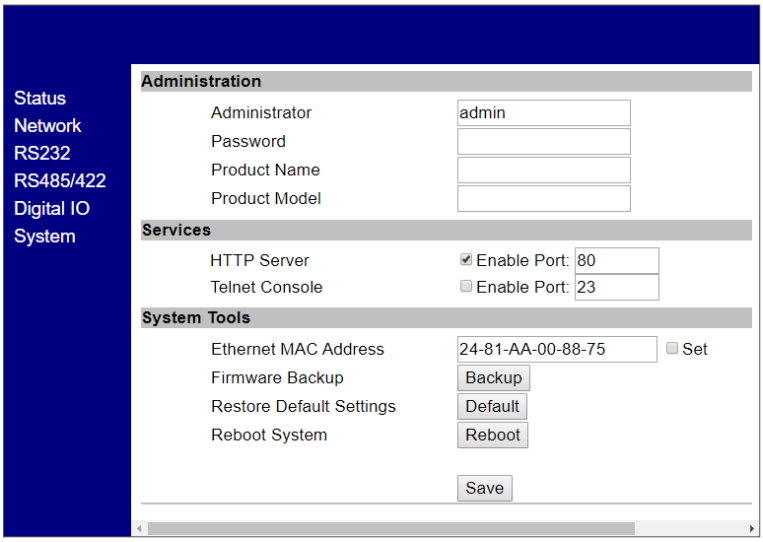
26.3 Status-Seite

» Auf der Status-Seite geben Sie zur Sicherheit ein Passwort ein. Dies ist optional und nicht unbedingt erforderlich. Der voreingestellte Administratorname für den Login ist „admin". Es ist kein Passwort vergeben.

- Der Product Name (Gerätename) kann frei konfiguriert werden, hat jedoch keinen Einfluss auf die Funktion des Gerätes.

- Das Login-password (Login-Passwort) schränkt den Zugang zur Konfigurationsseite des Gerätes ein.

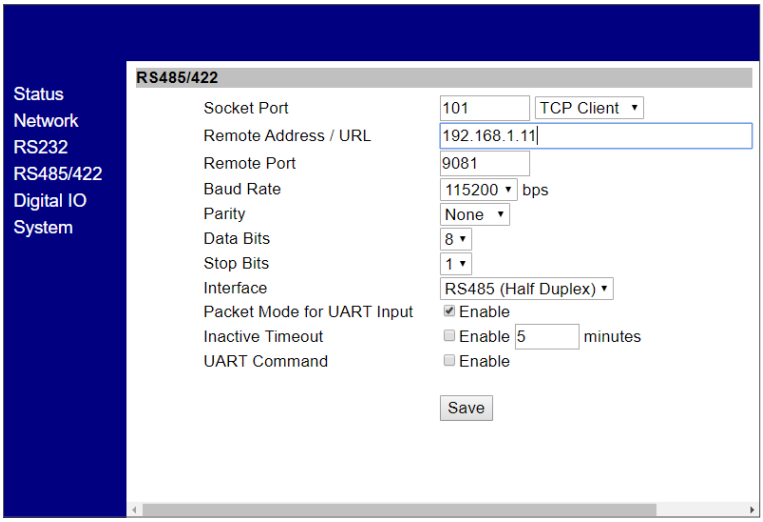
  Standardmäßig ist kein Passwort vergeben.



26.4 RS485/422

- Geben Sie im Feld „Remote Adresse /URL" die IP Adresse des PCs oder des Servers ein, auf dem die Xesar-Software installiert ist.

  Sie ist für die Kommunikation zwischen dem Xesar-Netzwerkadapter und der Xesar-Software verantwortlich. Wichtig ist, dass der Remote Port (standardmäßig 9081) gleichlautend, wie im Xesar-Installation Manager (OCH Port) angegeben ist.

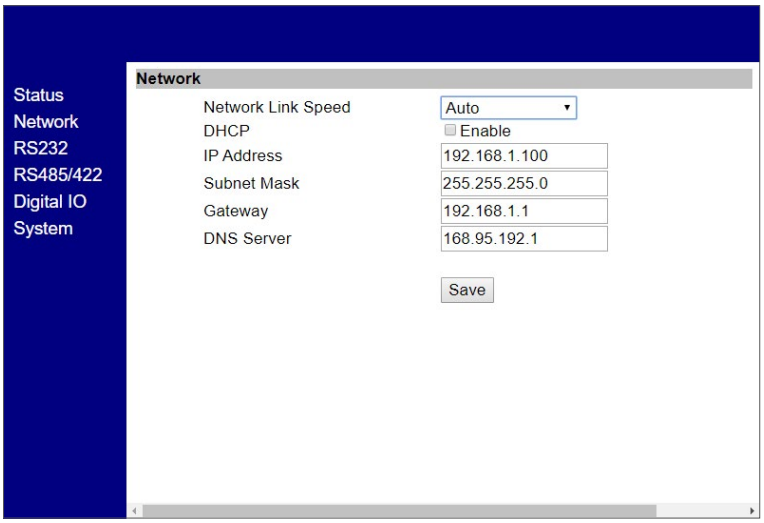


26.5 Network

» Auf der Network-Seite sollen die Felder, wie unten abgebildet, ausgefüllt werden.

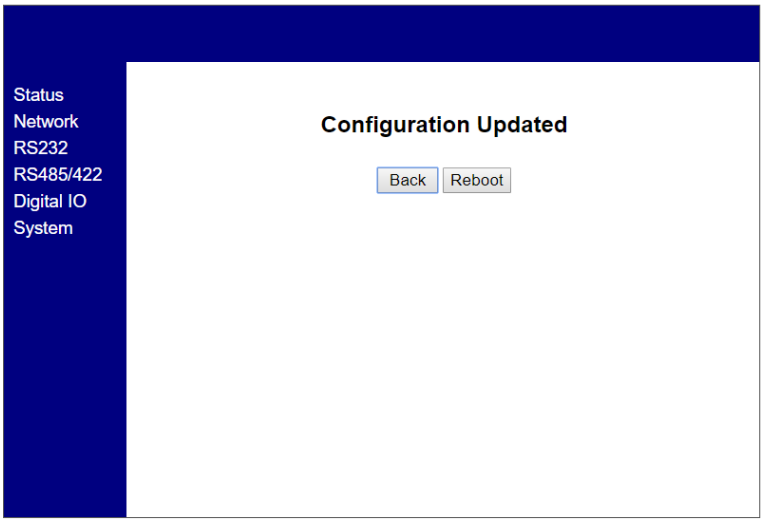
Die IP address (IP-Adresse) definiert die IP-Adresse des Xesar-Netzwerkadapters

Bitte beachten Sie: Wenn Sie diese Adresse ändern und auf **Save** klicken (oder mittels der ENTER-Taste bestätigen), kann der Netzwerkadapter nur noch über diese Adresse aufgerufen und konfiguriert werden.



» Klicken Sie nach Abschluss der Parametrierung auf **Save**, um die Konfiguration des Xesar-Netzwerkadapters abzuschließen

» Zum Übertragen der Daten an den Xesar-Ethernet Adapter drücken Sie „Reboot".



» Trennen Sie nach dem Rebooten des Netzwerkadapters den Xesar-Netzwerkadapter vom Konfigurations-PC.

» Schließen sie nun den Xesar-Netzwerkadapter an das Xeasar LAN Netzwerk an

Bei den bis zu **typisch 150** in einer Anlage möglichen Xesar-Netzwerkadaptern müssen Sie bis zu 150 verschiedene IP-Adressen definieren.

» Kontrollieren Sie auch die Netzwerkeinstellung des PC und beachten Sie den gültigen IP-Adressbereich Ihres Netzwerks.

- Die Subnet mask (Subnetzmaske) definiert das verwendete Subnetz.

- Die Remote Address /URL entspricht der IP-Adresse des Rechners, auf dem die Xesar-Software betrieben wird. Sie ist für die Kommunikation zwischen dem Xesar-Netzwerkadapter und der Xesar-Software verantwortlich.
  Wichtig ist, dass der Remote Port (standardmäßig 9081) gleichlautend wie im Xesar-Installation Manager (OCH Port) gegeben ist.

Die Remote-IP (PC) und IP address (Xesar-Netzwerkadapter) sind unterschiedlich! Sie müssen sich im gleichen Netzwerk befinden.

Beispielkonfiguration:

IP address	192.168.1.100
Subnet mask	255.255.255.0
Device Name	Adapter1
Login password	passwordadapater1
Remote IP	192.168.1.11

26.6 Reset eines Netzwerkadapters

Falls Sie Ihr gesetztes Passwort vergessen haben, oder der Xesar-Netzwerkadapter auf Grund von falschen Eingabedaten nicht funktioniert, können Sie den Xesar-Netzwerkadapter auf die Werkseinstellungen rücksetzen (Reset).

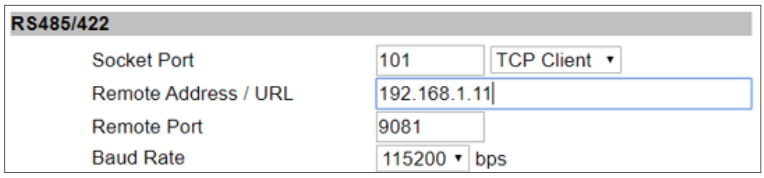
» Verbinden Sie das Netzgerät mit dem Xesar-Netzwerkadapter

» Drücken Sie den Reset-Knopf für mindestens 5 Sekunden.

Das Passwort und die Einstellungen werden auf die Werkseinstellungen zurückgesetzt.

» Wenn Sie im Fehlerfall einen Reset des Xesar-Netzwerkadapters durchführen, kontrollieren Sie anschließend noch einmal die **Parameter settings**.

Überprüfen Sie speziell den **Socket mode** (TCP Client), die **Baudrate** (115200) und den **Port** (9081= OCH Port im Installation-Manager)!



27 PC-Anlage: Offline-/Online-Betrieb

27.1 Anlage im Offline-Betrieb

Zutritte in Ihrer Anlage werden entsprechend auf den Zutrittsmedien definierten Berechtigungen ermöglicht. Die Xesar-Software muss zum Betrieb der Anlage nicht laufen.

Wenn Sie in Ihrer Anlage Änderungen durchführen wollen, müssen Sie die Xesar-Software starten und das Xesar-Dashboard aufrufen.

Änderungen, wie Berechtigungsänderungen von Personen oder Zutrittsmedien, Änderungen an Komponenten oder Änderungen in der Systemeinstellung können nur bei laufender Xesar-Software durchgeführt werden.

27.1.1 Xesar-Software starten

» Klicken Sie auf den **Installation-Manager-Button** auf Ihrem Desktop.
Der Installation-Manager wird gestartet und das Start-Fenster wird angezeigt.

» Klicken Sie im Start-Fenster auf den **Start-Button** der gewünschten Anlage.
Die Anlage wird gestartet und der Dashboard-Button wird aktiviert.

Mit dem Start der Anlage wird auch die angeschlossene Codierstation aktiviert und ist zum Verwalten der Zutrittsmedien bereit. (Das gilt nur für den Administrator-PC; für Client-PCs mit einer Codierstation ist die Installation und Verwendung des Periphery-Managers notwendig.)

» Klicken Sie auf den **aktivierten Dashboard-Button**.
Sie gelangen zur Login-Seite der Anlage.

» Melden Sie sich mit Ihrem **Benutzernamen** und Ihrem **Password** an.

Nach erfolgreichem Login können Sie die Anlage entsprechend Ihrer Benutzerrechte am Xesar-Dashboard verwalten.

27.1.2 Xesar-Software beenden

» Klicken Sie auf den **Beenden-Button**.
Zum Stoppen der Xesar-Software beenden Sie zuerst im Browser das Anlagen-Fenster durch Klick auf den Beenden-Button.

» Beenden Sie das Login-Fenster im Browser.

» Wechseln Sie zum Start-Fenster des Installation-Managers.

» Klicken Sie auf den **Stopp-Button der laufenden Anlage**.

Wenn Sie in den Einstellungen des Anlagen-Backups „Beim Stoppen der Anlage" gewählt haben, wird vor dem Stoppen dieses Backup durchgeführt.

Im Start-Fenster des Installation-Managers erkennen Sie eine gestoppte Anlage am angezeigten Start-Button.

Es kann immer nur eine Anlage gestartet werden und laufen.
Werden mehr als eine Anlage im Installation-Manager verwaltet, werden – sobald eine Anlage läuft – alle Start-Buttons der anderen Anlagen deaktiviert.

Im Offline-Betrieb gibt es keine Anzeige der laufenden Zutritte und des aktuellen Sicherheitszustandes der Anlage am Dashboard. Diese Funktionen sind nur im Online-Betrieb der Zutrittsanlage möglich.

27.2 Anlage im Online-Betrieb

Wenn Sie Ihre Anlage im Online-Betrieb betreiben, ist es notwendig, dass der Installation-Manager läuft und die Anlage gestartetet ist.

Im Online-Betrieb können Sie die laufenden Zutritte und den aktuellen Sicherheitszustand der Anlage überwachen und am Dashboard anzeigen. Dazu muss die Anlage im Online-Betrieb mit XVN und zumindest einem Online-Wandleser betrieben werden.

Personen haben nur entsprechend den auf den Zutrittsmedien definierten Berechtigungen Zutritt in der Anlage.

Änderungen, wie Berechtigungsänderungen von Personen oder Zutrittsmedien, Änderungen an Komponenten oder in den Systemeinstellungen können bei laufender Xesar-Software jederzeit am Dashboard durchgeführt werden.

27.2.1 Xesar-Software starten

» Klicken Sie auf den **Installation-Manager-Button** auf Ihrem Desktop.
Der Installation-Manager wird gestartet und das Start-Fenster wird angezeigt.

» Klicken Sie im Start-Fenster auf den **Start-Button**.
Die gewünschte Anlage wird gestartet und der Dashboard-Button wird aktiviert.

Mit dem Start der Anlage wird auch die angeschlossene Codierstation aktiviert und ist zum Verwalten der Zutrittsmedien bereit. (Das gilt nur für den Administrator-PC; für Client-PCs mit einer Codierstation ist die Installation und Verwendung des Periphery-Managers notwendig.)

» Klicken Sie auf den **aktivierten Dashboard-Button.**
Sie gelangen zur Login-Seite der Anlage.

» Melden Sie sich mit Ihrem **Benutzernamen** und Ihrem **Password** an.

Nach erfolgreichem Login können Sie die Anlage entsprechend Ihrer Benutzerrechte am Anlagen-Dashboard verwalten.

27.2.2 Xesar-Software beenden

» Klicken Sie auf den **Beenden-Button** .
Zum Stoppen der Xesar-Software beenden Sie zuerst im Browser das Anlagen-Fenster durch Klick auf den Beenden-Button.

» Beenden sie das Login-Fenster im Browser.

» Wechseln Sie zum Start-Fenster des Installation-Managers.

» Klicken Sie auf den **Stop-Button der laufenden Anlage**.

Wenn Sie in den Einstellungen des Anlagen-Backups „Beim Stoppen der Anlage" gewählt haben, wird vor dem Stoppen dieses Update durchgeführt.

Im Start-Fenster des Installation-Managers erkennen Sie eine gestoppte Anlage am angezeigten Start-Button.

Es kann immer nur eine Anlage gestartet werden und laufen.
Werden mehr als eine Anlage im Installation-Manager verwaltet, werden, sobald eine Anlage läuft, alle Start-Buttons der anderen Anlagen deaktiviert.

Im Offline-Betrieb gibt es keine Anzeige der laufenden Zutritte und des aktuellen Sicherheitszustandes der Anlage am Dashboard. Diese Funktionen sind nur im Online-Betrieb der Zutrittsanlage möglich.

27.3 PC-Anlage im Mehrplatzbetrieb

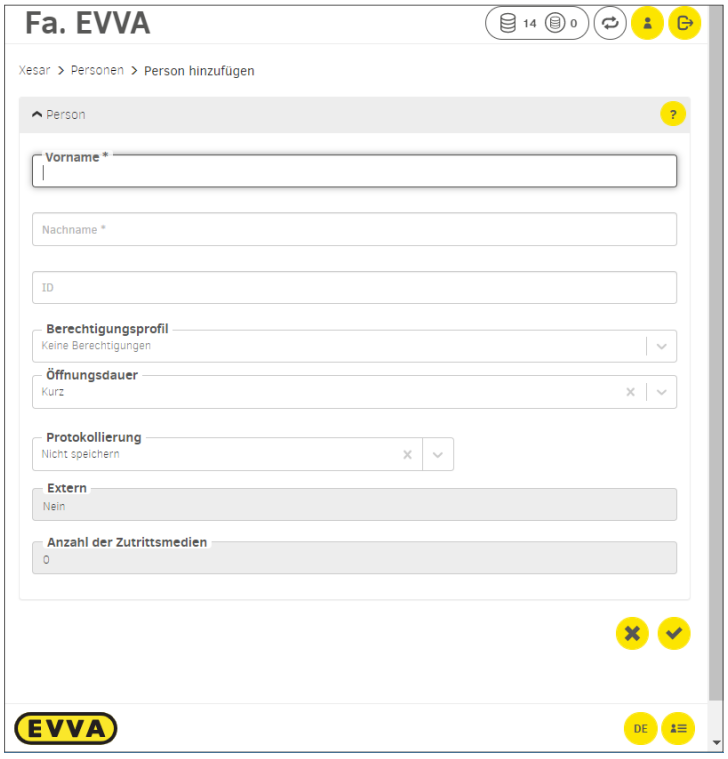
PC-Anlagen können auch im Mehrplatzbetrieb verwaltet werden. Dazu müssen sich die Client-PCs im selben Netzwerk wie der Administrator-PC (PC mit installierter Xesar-Software) befinden und sich im Browser über die IP-Adresse und Port mit dem Administrator-PC verbinden. Nach erfolgreichem Login können die Client-PCs die Anlage verwalten und bedienen.

Zum Verwalten von Zutrittsmedien auf einem Client-PC ist eine externe Codierstation notwendig. Für den Betrieb der Codierstation muss der Periphery-Manager installiert, gestartet und am verwendeten Browserfenster aktiviert werden.

28 Xesar Kurzanleitung

28.1 Person hinzufügen

Ein neuer Mitarbeiter tritt in Ihr Unternehmen ein:



- Wählen Sie die Kachel **Personen** aus.
- Klicken Sie auf das **Plus-Symbol.**
- Pflichtfelder* müssen ausgefüllt werden (Vor- und Nachname).
- ID eingeben (z. B. Personalnummer).

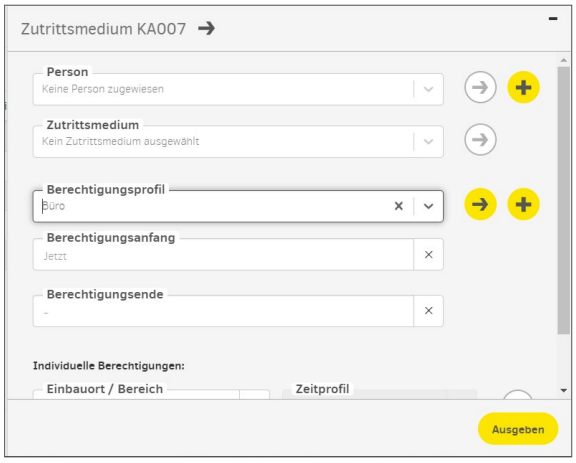
Optionale Komfortfunktionen:

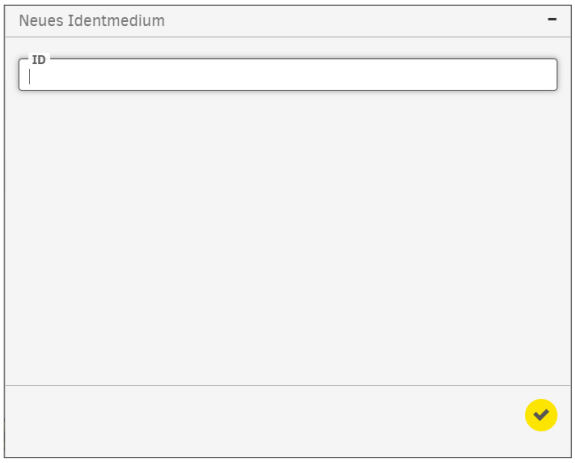
- Freigabedauer:
  Kurz/Lang (z. B. für Personen mit Handicap)
- Protokollierung:
  Nicht speichern / Zeitlich begrenzt speichern / Unbegrenzt speichern
- Wenn gewünscht, können bereits definierte Berechtigungen (Berechtigungsprofile) für neu angelegte Personen ausgewählt werden.
- Individuelle Berechtigungen werden in späterer Folge beim Zutrittsmedium vergeben.

Bei Bedarf können Sie einer Person mehrere Zutrittsmedien zuweisen.

28.2 Zutrittsmedium ausgeben

Um ein neues Zutrittsmedium auszugeben, legen Sie es auf die Codierstation. Es öffnet sich ein Pop-Up-Fenster. Sie können optional eine Identifikationsnummer (ID) vergeben.





Zutrittsmedien müssen nicht zwangsläufig einer Person zugewiesen werden. Das ist ideal für den Zutritt von externen Unternehmen mit wechselndem Personal.

- **Optional:** Wählen Sie beim Zutrittsmedium eine Person aus.
- Wählen Sie ein Berechtigungsprofil aus.
- **Wenn Sie den Berechtigungszeitraum einschränken wollen**, ändern Sie den Berechtigungsanfang und das Berechtigungsende des Zutrittsmediums.
- **Optional:** Wählen Sie individuellen Zugang zu bestimmten Einbauorten aus, z. B. Garderobekasten.
- Geben Sie das Zutrittsmedium aus.

Ein Ausgabeprotokoll mit den Daten zum Zeitpunkt der Ausgabe wird erstellt.

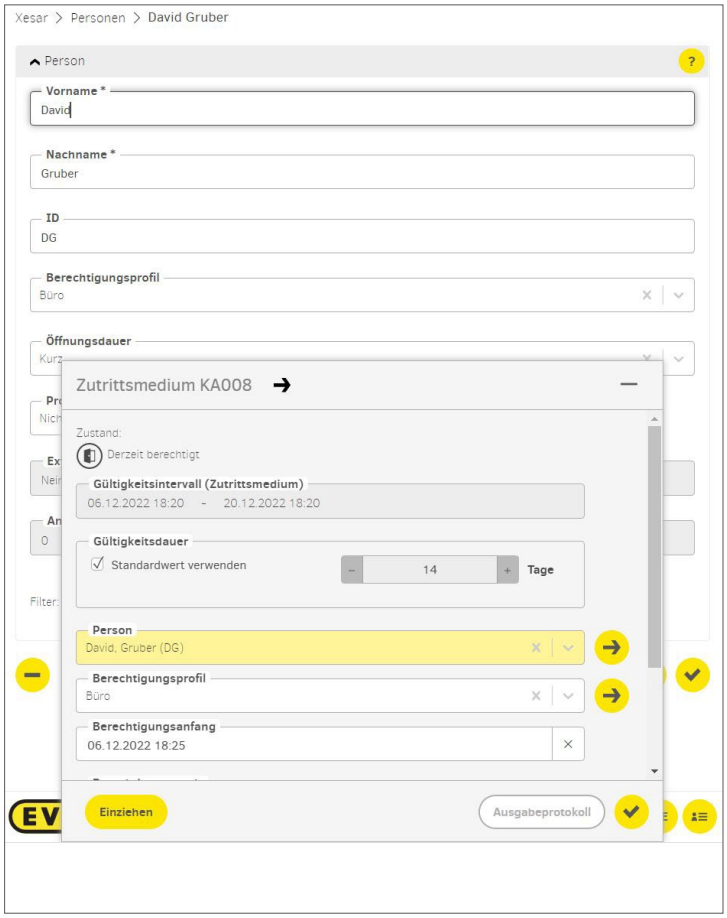
- Drucken Sie das Ausgabeprotokoll aus und lassen Sie die Übernahme des Zutrittsmediums von der zugewiesenen Person bestätigen.

Die Rücknahme des Zutrittsmediums kann auf dem Ausgabeprotokoll bestätigt werden.

Bei Bedarf können Sie einer Person mehrere Zutrittsmedien zuweisen.

Wenn Sie das Bezahlmodell Stück KeyCredits verwenden, klicken Sie auf den Button **Abbuchen**  , um die Berechtigungsänderung zu bestätigen. Bei dem Bezahlmodell KeyCredit Xesar Lifetime sind neue Zutrittsmedien und Berechtigungsänderungen inkludiert.

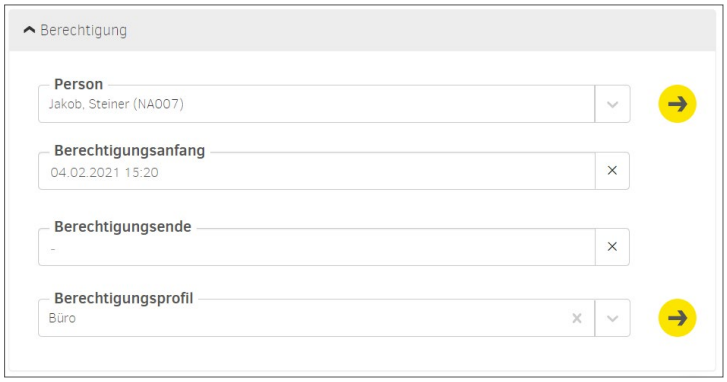
28.3 Einfache Methode: Zutrittsmedien einer Person zuweisen



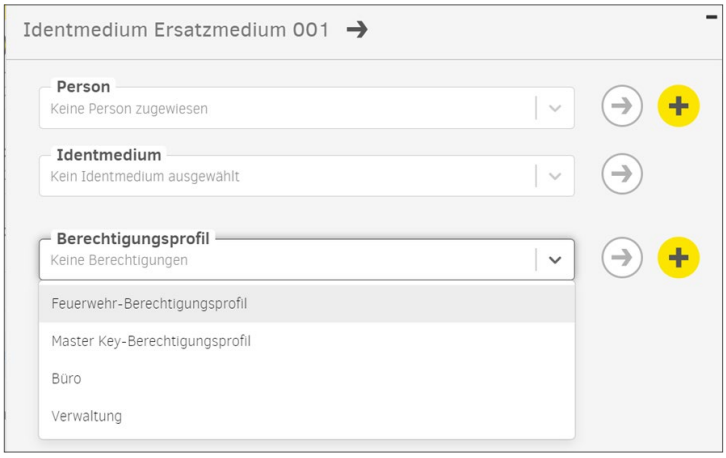
- Öffnen Sie die Personendetailseite der gewünschten Person.
- Legen Sie ein neues Zutrittsmedium auf die Codierstation.
- Im Overlay-Fenster wird der Personenname mit dem Berechtigungsprofil automatisch eingefügt.
- Bestätigen Sie die Eingabe im Overlay-Fenster.
- Bei Bedarf kann ein Ausgabeprotokoll erstellt werden.

28.4 Berechtigungsprofile ändern, hinzufügen oder löschen

Ein Mitarbeiter wechselt in eine andere Abteilung und benötigt das entsprechende Berechtigungsprofil:



- Klicken Sie auf die Dashboard-Kachel **Zutrittsmedien**:
  Berechtigungsprofile und individuelle Berechtigungen für Zutrittsmedien können unter der Dashboard-Kachel „Zutrittsmedien" in der jeweiligen Zutrittsmedien-Detailansicht ausgewählt und geändert werden.
- Legen Sie nach der Änderung das Zutrittsmedium auf die Codierstation, um das Zutrittsmedium zu aktualisieren.



- Berechtigungsprofile und individuelle Berechtigungen können auch direkt durch Auflegen des Zutrittsmediums auf die Codierstation im angezeigten Fenster ausgewählt oder geändert werden.

Sonderfall: Feuerwehr und Generalhauptschlüssel
Im Bedarfsfall kann einem Zutrittsmedium ein Generalhauptschlüssel- oder ein Feuerwehr-Berechtigungsprofil zugewiesen werden.

Ein Zutrittsmedium mit **Feuerwehr-Berechtigungsprofil** hat **zeitlich unbegrenzt** zu jeder Tür Ihrer Anlage Zutritt.
Ein Zutrittsmedium mit **Generalhauptschlüssel-Berechtigungsprofil** hat zu jeder Tür Ihrer Anlage Zutritt und kann **in der Gültigkeitsdauer begrenzt** werden. Nach Ablauf der Gültigkeitsdauer muss das Zutrittsmedium wieder aktualisiert werden.

Bewahren Sie Zutrittsmedien mit Feuerwehr- oder Generalhauptschlüssel-Berechtigung besonders sicher und sorgfältig auf.

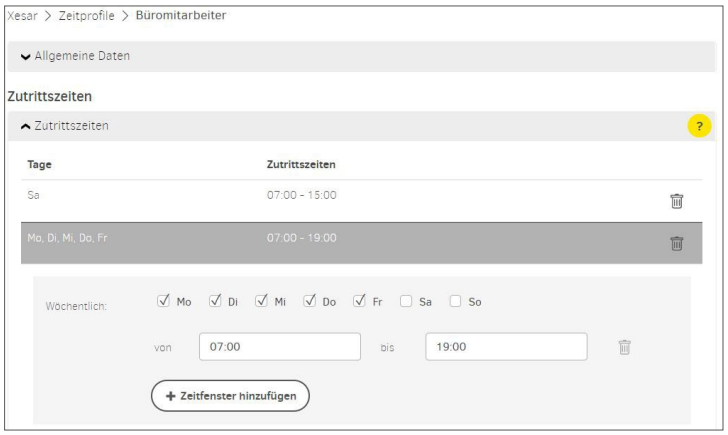
Es können in einer Anlage nur maximal je 15 Medien mit einem Feuerwehr– oder Generalhaupschlüssel-Berechtigungsprofil ausgestellt werden.

Eine detaillierte Beschreibung zum Thema „Berechtigungsprofile" finden Sie im Xesar-Systemhandbuch.

28.5 Zeitprofile ändern

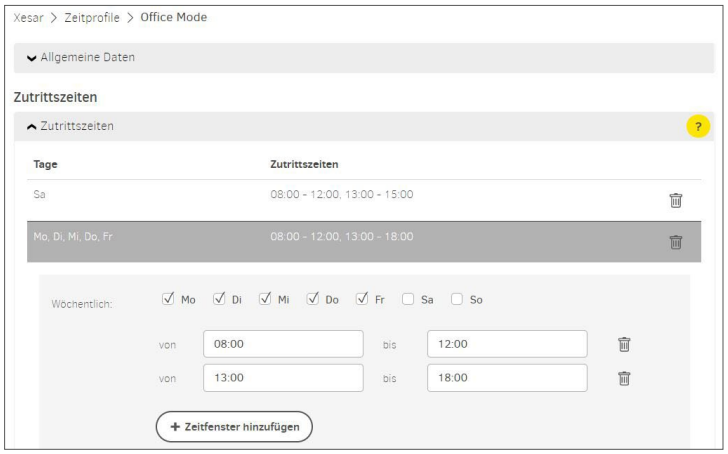
Eine Person erhält zu geänderten Zeiten Zutrittsberechtigungen.
Die Öffnungszeiten des Verkaufslokals haben sich geändert.

Zeitprofil



» Zeitfenster für den Zutritt ändern
Wenn sich für eine Person oder eine Personengruppe die Arbeitszeit ändert, müssen die Zeitfenster für den Zutritt der Person bzw. Personengruppe geändert werden.

Office-Mode-Zeitprofil



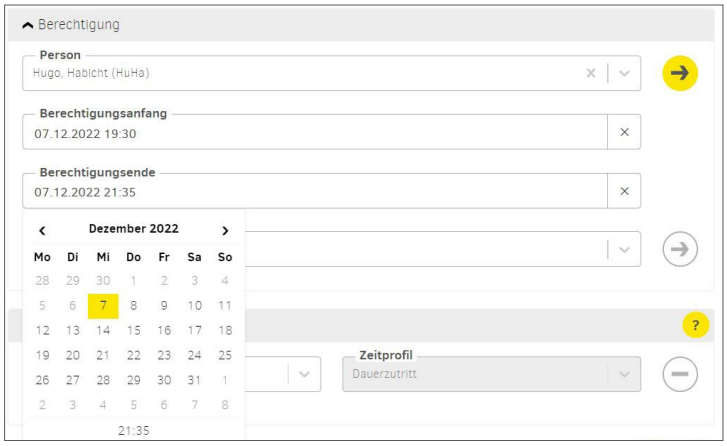
» Eine Komponente soll zu einem bestimmten Zeitpunkt in Daueröffnungsbetrieb schalten und zu einem bestimmten Zeitpunkt schließen.

Eine detaillierte Beschreibung zum Thema „Zeitprofile" finden Sie im Xesar-Systemhandbuch.

Die Eingabe der Zeiten in den Eingabefeldern kann numerisch oder mittels Pfeiltasten erfolgen.

28.6 Zutrittsmedien inaktiv setzen

Wenn die Zutrittsberechtigung einer Person für längere Zeit unterbrochen werden soll, kann das Zutrittsmedium deaktiviert werden. Dabei bleibt das Medium mit dem Berechtigungsprofil der Person zugewiesen. Der Zutritt wird durch Setzen des Berechtigungsende auf den aktuellen Zeitpunkt bis auf weiteres deaktiviert.



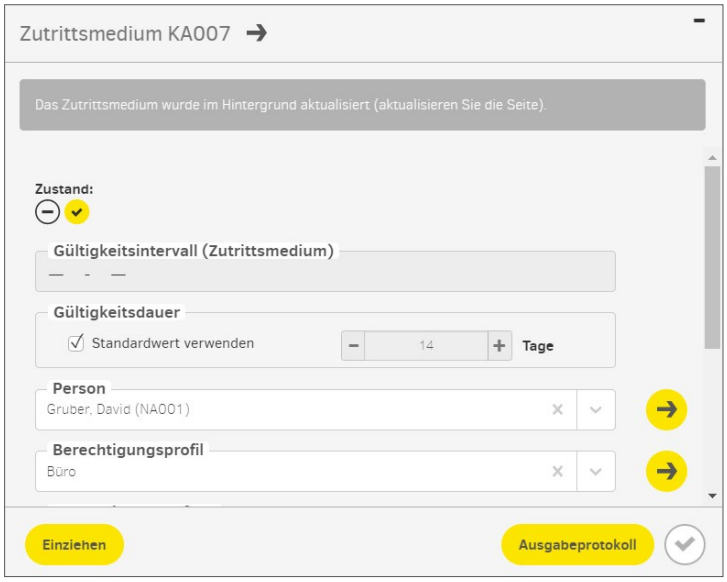
- Öffnen Sie die Detailseite des Zutrittsmediums, das inaktiv gesetzt werden soll.
- Klicken Sie auf das aktuelle Berechtigungsende (Datum mit Uhrzeit, z. B.7.12. um 21:35). Das Medium wird sofort inaktiv gesetzt.
- Anschließend aktualisieren Sie das Medium am Online-Wandleser oder an der Codierstation, damit es zur Anlage keinen Zutritt mehr hat.

Die Zutrittsberechtigung am Medium kann durch Setzen eines neuen Berechtigungsende-Zeitpunkts und Aktualisierung am Online-Wandleser oder an der Codierstation wieder aktiviert werden.

Bei diesem Vorgang werden keine Blacklisteinträge in der Anlage erzeugt.

28.7 Zutrittsmedium einziehen

Ein Zutrittsmedium einziehen und später in der Anlage erneut verwenden, z. B. Mitarbeiter verlässt das Unternehmen.



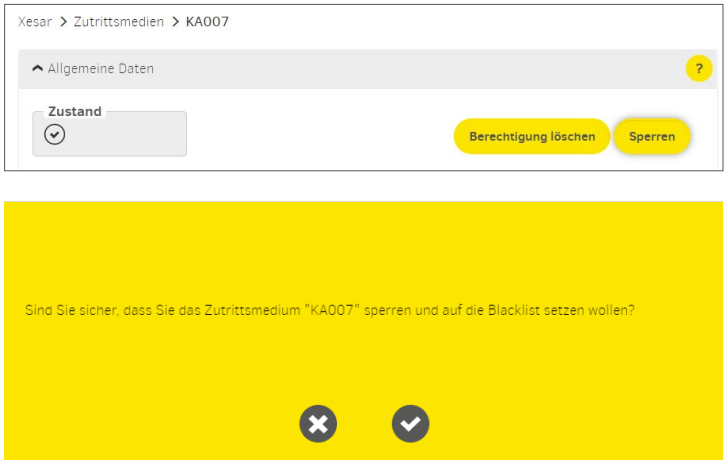
» Legen Sie das Zutrittsmedium auf die Codierstation.
» Wählen Sie **Einziehen**.

Nach dem Einziehen kann das Zutrittsmedium ausschließlich in dieser Anlage wiederverwendet werden und wird als neues Zutrittsmedium angezeigt, sobald es erneut auf die Codierstation gelegt wird.

Eine detaillierte Beschreibung zum Thema „Medium einziehen" finden Sie im Xesar-Systemhandbuch.

28.8 Zutrittsmedium sperren

Ein Zutrittsmedium wurde verloren oder gestohlen.
Damit die Anlage vor unberechtigtem Zutritt geschützt wird, muss das Zutrittsmedium gesperrt werden.



28.8.1 Zutrittsmedium sperren

- Wählen Sie die Kachel **Zutrittsmedium** aus.
- Wählen Sie das zu sperrende Zutrittsmedium aus und klicken Sie auf **Sperren**.

Die Xesar-Software erzeugt eine Blacklist und Wartungsaufgaben für alle Komponenten der gefährdeten Einbauorte.

- Synchronisieren Sie das Xesar-Tablet und führen Sie die Wartungsaufgaben an den Komponenten aus.
- Alternativ kann mittels Zutrittsmedien die Blacklist an die Komponenten verteilt werden.
- Delete-Key-Funktion – an synchronisierten Xesar-Komponenten mit der aktuellen Blacklist wird das gesperrte Zutrittsmedium endgültig deaktiviert.

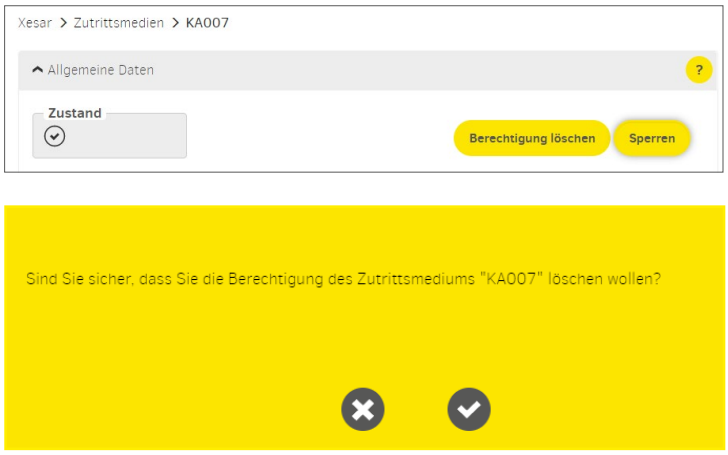
28.8.2 Berechtigungen löschen

Einem vorhandenem Zutrittsmedium können die Berechtigungen entzogen werden.

- Die Berechtigungen am Zutrittsmedium werden gelöscht.
- Es wird kein Blacklisteintrag und keine Wartungsaufgaben erzeugt.
- Das Zutrittsmedium bleibt der Person zugewiesen.
- Es können neue Berechtigungen vergeben werden.

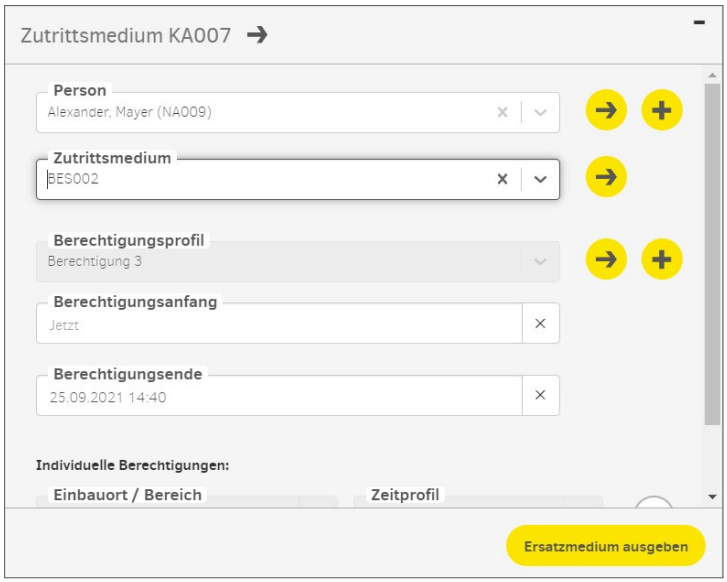
» **Zutrittsmedium aktualisieren**
Zum Aktualisieren muss das Zutrittsmedium am Online-Wandleser angehalten oder auf die Codierstation gelegt werden.

Eine detaillierte Beschreibung zum Thema „Zutrittsmedium sperren" finden Sie im Xesar-Systemhandbuch.



28.9 Ersatzmedium ausstellen

Das Zutrittsmedium wurde zu Hause vergessen – ein Ersatzmedium wird ausgestellt.



- Legen Sie ein neues Zutrittsmedium auf die Codierstation.
- Wählen Sie im Drop-Down Feld „Person" die Person aus, für die ein Ersatzmedium ausgestellt werden soll.
- Wählen Sie im Drop-Down Feld „Zutrittsmedium" das zu ersetzende Zutrittsmedium aus.
- Klicken Sie auf **Ersatzmedium ausgeben**.

Das Ersatzmedium hat jetzt für die eingestellte Berechtigungsdauer die Berechtigungen des Originalmediums.

- Die Berechtigungsdauer für Ersatzmedien kann unter der Kachel **Einstellungen** in der Xesar-Software eingestellt werden.

Beachten Sie, dass das Originalmedium weiterhin gültig ist.

Für Hilfe und weitere Informationen wenden Sie sich an Ihren EVVA Partner oder das Technische Büro von EVVA.

Eine detaillierte Beschreibung zum Vorgang „Ersatzmedium ausstellen" finden Sie im Xesar-Systemhandbuch.

www.evva.com