

Xesar

Systemhandbuch | 3.0.2xx

Inhaltsverzeichnis

1	EINLEITUNG	7
1.1	Allgemeine rechtliche Hinweise	7
1.2	Impressum	8
1.3	Zeichenerklärung	9
1.4	Zeichenerklärung Xesar-Software	9
1.4.1	Allgemein	9
1.4.2	Zustände Identmedien	12
2	HARDWARE UND MONTAGE	13
2.1	Xesar-Zutrittskomponenten	13
2.1.1	Xesar-Beschlag	15
2.1.2	Xesar-Drücker	18
2.1.3	Xesar-Zylinder	21
2.1.4	Xesar-Hangschloss	24
2.1.5	Xesar-Wandleser	26
2.2	Montage der Xesar-Zutrittskomponenten	30
2.3	Ereignissignalisierung	32
2.4	Codierstation und Mini-Codierstation	33
2.5	Xesar-Tablet	34
2.6	Xesar-Notstromgerät	37
2.7	AdminCard	38
2.8	Xesar-Identmedien	39
2.9	Construction-Card	40
3	SYSTEMANFORDERUNGEN	41
3.1	Xesar 3.0 – Einplatzanlage	41
3.1.1	Systemanforderungen Einplatzanlage	42
3.1.2	Bereitgestellte Services im Internet	43
3.2	Xesar 3.0 – Server Mehrplatzanlagen	44

3.2.1	Systemanforderungen Server	45
3.2.2	Getestete Betriebssysteme	45
3.2.3	Nicht getestete Betriebssysteme	46
3.2.4	Systemanforderungen Admin-PC mit Codierstation und AdminCard	47
3.2.5	PC Betriebssysteme:	48
3.2.6	Systemanforderung Client-PC mit Codierstation ohne AdminCard	49
3.2.7	Betriebssysteme:	50
3.2.8	Systemanforderungen Client PC ohne Codierstation (PC/Tablet/Smartphone)	50
3.2.9	Betriebssysteme:	51
3.2.10	Systemanforderungen Netzwerk (Lokales Netzwerk und Internet)	52
3.2.11	Bereitgestellte Services im Internet	52
3.2.12	Bereitgestellte Services im lokalen Netzwerk	53
3.3	Anhang	53
3.4	Service Katalog: Server-Kommunikation	54
3.5	Service Katalog: Kommunikation Client-PC – Server (Backend)	55
3.6	Kommunikation Online Wandleser – Server (Backend)	56
4	ANLAGENINSTALLATION UPGRADE UND UPDATES	57
4.1	Upgrade von Xesar 2.2 auf Xesar 3.0	57
4.1.1	Upgrade-Kompatibilität von Xesar	58
4.1.2	Anleitung für Upgrade Xesar 2.2 auf Xesar 3.0	58
4.2	Vorbereitung des PCs für die Xesar 3.0-Installation	60
4.2.1	Docker Installation	60
4.2.2	Download Docker	61
4.2.3	Docker installieren	61
4.2.4	Installation des Treibers für die Codierstation	66
4.2.5	Automatische Treibersuche über Windows	66
4.2.6	Manuelle Treibersuche auf der Homepage des Herstellers	69
5	XESAR 3.0 PROGRAMME	74
5.1	Xesar-Installation Manager	76

5.2	AdminCard – Tausch	91
5.3	Xesar-Software Update.....	92
5.3.1	Xesar-Installation Manager Update.....	97
5.4	Xesar-Periphery Manager.....	98
5.5	Codierstation mit der Xesar-Software verknüpfen	103
5.6	Xesar-Tablet in Anlage einbinden	109
5.7	Manuelle Deinstallation und Installation der Xesar-App.....	115
6	SICHERUNG DER XESAR-ANLAGENDATEN IM XESAR-INSTALLATION MANAGER.....	122
6.1	Manuelles Backup	122
6.2	Automatisches Backup.....	124
6.3	Backup Files.....	125
6.4	Restore	126
7	INBETRIEBNAHME XESAR-SOFTWARE	132
7.1	Allgemeines zur Inbetriebnahme	132
7.2	Einstellungen	133
7.2.1	Sicherheitseinstellungen	133
7.2.2	Gültigkeits- und Berechtigungsdauer der Identmedien	133
7.2.3	Systemeinstellungen	135
7.3	Benutzergruppen	137
7.4	Benutzer	142
7.5	Kalender.....	145
7.6	Zeitprofile.....	147
7.6.1	Office Mode Zeitprofil hinzufügen	150
7.6.2	Zeitprofil hinzufügen	152
7.7	Einbauorte	153
7.7.1	Einbauort hinzufügen:	154
7.7.2	Einbauort beschreiben	154

7.8	Bereiche	156
7.9	Berechtigungsprofile	158
7.10	Personen	161
7.10.1	Person hinzufügen	162
7.11	Identmedien	164
7.11.1	Neues Identmedium	164
7.11.2	Vorhandenes Identmedium	166
7.12	Xesar-Zutrittskomponente taufen	169
7.13	Inbetriebnahme des Xesar-Online Wandlerer Netzwerkadapters EXPERT EX9132CST	170
7.13.1	PC-Konfiguration	170
7.13.2	Inbetriebnahme eines Xesar-Netzwerkadapters	172
7.13.3	Status-Seite	173
7.13.4	RS485/422	174
7.13.5	Network	174
7.13.6	Reset eines Netzwerkadapters	176
8	XESAR-SYSTEMVERWALTUNG	177
8.1	Starten und Beenden von Xesar	177
8.2	Das Xesar-Dashboard	178
8.3	Die Listen-Filterfunktion	179
8.3.1	Manuell filtern	179
8.3.2	Filter-Presets	179
8.3.3	Spaltenansicht	180
8.4	Mein Profil	181
8.5	KreyCredits (Stück)	182
8.6	Support	184
8.6.1	Über Xesar	184
8.6.2	Xesar-Hilfe	185
8.6.3	Aktualisierung	185
8.6.4	Supportinformationen herunterladen	185
9	WARTUNGS- UND KONFIGURATIONSAUFGABEN	187
9.1	Firmware Update	188
9.2	Batteriewarnung	189

9.3	Codierstationen	189
9.4	Online-Störung	190
9.5	Identmedien	191
9.5.2	Identmedium einziehen	192
9.5.3	Identmedium Berechtigung entziehen	193
9.5.4	Identmedium sperren (auf Blacklist setzen)	193
9.5.5	Nicht schreibbare Identmedien	194
9.5.6	Unsichere Identmedien	195
9.5.7	Identmedien nicht aktuell	195
9.5.8	Freigaben mit gesperrten Identmedien.....	196
9.6	Protokolle	196
9.6.1	Ereignisprotokoll	196
9.7	Xesar-Tablet (Programmiergerät)	198
9.7.1	Xesar-Tablet App	198
9.7.2	Firmware-Update	200
9.7.3	Batteriestatus der Xesar-Zutrittskomponente	200
9.7.4	Xesar-Zutrittskomponente taufen	201
9.8	Xesar-Virtuelles Netzwerk (XVN)	202
9.8.1	Übertragung von Zutrittsereignissen über die Identmedien	202
9.8.2	Übertragung von Blacklisteinträgen über die Identmedien.....	203
9.8.3	Übertragung der Information Öffnung durch gesperrtes Medium	203
9.8.4	Übertragung der Information Identmedium von Türkomponente gelöscht	204
9.8.5	Übertragung des Batteriestatus über die Identmedien	205
9.9	AdminCard ersetzen	205
9.10	Komponente hinzufügen rückgängig machen	207
9.11	Komponente ausbauen (Rücksetzen in Baustellenmodus)	208
9.12	Komponente erzwungen ausbauen (Komponente defekt)	209
9.13	Xesar-Online Wandler	209
9.14	Mögliche Fehler, die auftreten können.....	211
10	ABBILDUNGSVERZEICHNIS.....	217

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 des Xesar-Schließsystems gesetzliche, insbesondere datenschutzrechtliche Genehmigungs-, Melde- und Registrierungspflichten (zB 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.



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 Xesar-Produktkatalog:



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

1.2 Impressum

Version: 09/2019 Deutsch

Mit dem Erscheinen eines neuen Systemhandbuchs verliert diese Ausgabe ihre Gültigkeit.

Alle Rechte vorbehalten. Ohne schriftliche Zustimmung des Herausgebers darf dieses Systemhandbuch, auch nicht auszugsweise, in irgendeiner Form reproduziert oder unter Verwendung elektronischer, mechanischer oder chemischer Verfahren vervielfältigt oder verarbeitet werden.

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

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


SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden
Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

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
	Optionen
	Links
	Schritt bei Handlungsanweisungen

Tabelle 1: Zeichenerklärung

1.4 Zeichenerklärung Xesar-Software

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

1.4.1 Allgemein

#	Zustand	Visualisierung	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 Xesar-Anlage, Zeitprofil oder Einbauort

#	Zustand	Visualisierung	Erklärung
5	Bearbeiten		Bearbeiten der Anlage (Xesar-Installation Manager)
6	Anwendung starten		Starten der Anlage (Xesar-Installation Manager) oder Starten der Verbindung zwischen Codierstation und Xesar-Software (Xesar-Periphery Manager)
7	Anwendung stoppen		Stoppen der Anlage (Xesar-Installation Manger) oder Stoppen der Verbindung zwischen Codierstation und Xesar-Software (Xesar-Periphery Manager)
8	Download		Download von z. B. der Xesar-Tablet-App oder des Xesar-Periphery Managers
9	Weiter		Weiter zur nächsten Eingabe
10	Laden / Übertragen		Lader der Amincard
11	Exportieren		Exportieren von Listen (z. B. Personen oder Ereignisse)
12	Filtern		Anzeige möglicher Filter-Einstellungen der Funktion
13	Aktualisieren / Verbinden		Am Xesar-Dashboard wird im Backend eine Aufgabe durchgeführt
14	Nicht aktualisiert / warten auf Aktualisierung / Update downloaden		Ein Update ist verfügbar und kann heruntergeladen werden
15	Suchen		Suchen nach einem speziellen Ereignisbeitrag
16	Ausklappen		Das Sichtfeld erweitern
17	Einklappen		Das Sichtfeld reduzieren
18	Gehe zu		Das Browserfenster für die Xesar-Verwaltungssoftware öffnen
19	Systemprotokoll		Alle Aktionen anzeigen, die in der Xesar-Software von Benutzern und vom System durchgeführt worden sind

#	Zustand	Visualisierung	Erklärung
20	Gefiltert nach Bereichen		Zeigt alle Bereiche an, zu welchen eine Person eine Zutrittsberechtigung hat
21	Gefiltert nach Einbauorten		Zeigt alle Einbauorte an, zu welchen eine Person eine Zutrittsberechtigung hat
22	Gefiltert nach Identmedien		Zeigt alle Identmedien an, die einer Person zugewiesen sind
23	Gefiltert nach Personen		Filtern nach Personen
24	Mein Profil		Profil bearbeiten: Beschreibung hinzufügen und persönliches Passwort ändern
25	Angezeigte Sprache		Spracheinstellung ändern
26	Anzeige Stück KeyCredits		Anzeige der abzubuchenden KeyCredits (z. B. durch Berechtigungsänderungen oder Ausgabe von neuen Identmedien)
27	Anzeige KeyCredit Xesar-Lifetime		Wird angezeigt, wenn KeyCredit Xesar-Lifetime eingelöst wurde
28	Ereignisprotokoll		Anzeige Ereignisse, z. B. unter einer Person (es werden alle Zutrittsereignisse der Person gefiltert angezeigt)
29	Hilfetexte	 	Anzeige von Hilfetexten
30	Listenexport	 	Die angezeigte Liste als csv-Datei oder als xls-Datei exportieren
31	Listenansichtseinstellung		Darstellung der Liste anpassen (Spaltenauswahl, Zeilenanzahl pro Seite, Einstellungen speichern und Zurücksetzen)
32	Backup-Button		Im Xesar-Installation Manager wird ein Backup der Anlagendaten erstellt
33	Logout		Sitzung beenden

Tabelle 2: Zeichenerklärung Xesar-Software

1.4.2 Zustände Identmedien

#	Zustand	Visualisierung	Erklärung
1	Unsicher gesperrtes Identmedium		Noch unsichere Einbauorte vorhanden
2	Sicher gesperrtes Identmedium		Keine unsicheren Einbauorte vorhanden
3	Unberechtigtes Identmedium		Das Identmedium verfügt über keine Berechtigung
4	Aktuell gültig		
5	Aktuell ungültig		
6	Aktuell gültiges Identmedium wird bei Aktualisierung zu einem ungültigen Identmedium	 	
7	Aktuell ungültiges Identmedium wird bei Aktualisierung zu einem gültigen Identmedium	 	
8	Aktuell ungültiges Identmedium mit einem Gültigkeitsintervall auf dem Identmedium, das in der Zukunft liegt	 	
9	Deaktiviertes Identmedium		Das Medium wurde deaktiviert; es gibt keine unsicheren Einbauorte mehr; der Kalender spielt keine Rolle mehr.

Tabelle 3: Zeichenerklärung Identmedien

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

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/>



Abbildung 1: Systemarchitektur (Symbolfoto)

2.1 Xesar-Zutrittskomponenten

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



Xesar-Beschlag



Xesar-Drücker



Xesar-Zylinder



Xesar-Hangschloss



Xesar-Wandleser

Abbildung 2: Xesar-Zutrittskomponenten (Symbolfotos)

Jede Xesar-Zutrittskomponente verfügt über eine Stecker-Schnittstelle, die zur Aktualisierung mit dem Tablet dient. Die Stecker-Schnittstelle kann bei batteriebetriebenen Xesar-Zutrittskomponente bei Bedarf auch für die Notstromversorgung benutzt werden.

Die Stecker-Schnittstelle befindet sich auf der Vorderseite der Xesar-Zutrittskomponente, hinter dem EVVA-Logo (Stecker-Abdeckung).



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 die Stecker-Abdeckung nach vorne.



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

2.1.1 Xesar-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


SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service



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



Abbildung 3: Xesar-Beschlag (Symbolfoto)

- ① Optische Signalisierung
- ② Leseinheit
- ③ Stecker-Schnittstelle (EVVA-Logo)
- ④ Drücker

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

Der Xesar-Beschlag signalisiert Ereignisse sowohl akustisch als auch optisch. Beachten Sie die Liste der unterschiedlichen akustischen und optischen Signale im Kapitel 2.2 Ereignissignalisierung.

Der Xesar-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 Identmedium an der Leseinheit vorgehalten, wird der Außendrücker für 5 Sekunden mechatronisch eingekuppelt. Wird jetzt der Außendrücker betätigt, wird die Falle bzw. der Riegel – abhängig von der Schlosstypen – 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 Xesar-Beschlags führen!

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

Wenn Signal „Batterie schwach“ angezeigt wird, müssen die Batterien umgehend gewechselt werden. (Wenn das Signal „Batterie schwach“ 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 dazu das Kapitel 2.2 Montage der Xesar-Zutrittskomponenten.



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 Xesar-Beschlag mit dem Xesar-Tablet synchronisiert werden!

Der Batteriewechsel des Xesar-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 Xesar-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 2.2. Montage der Xesar-Systemkomponenten.

- » Setzen Sie das Innenschild wieder auf das Befestigungsblech.
Schieben Sie das Innenschild über den Drücker.
- » Ziehen Sie die Schraube an der Unterseite des Xesar-Beschlags mit einem Torx-Schraubendreher T8 an.

2.1.2 Xesar-Drücker

- Batteriebetriebene Zutrittskomponente
- Einsatz im Innenbereich

- Geeignet für Vollblattdüren mit gängigen Vollblattdürschlössern 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 Xesar-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.



Abbildung 4: Xesar-Drücker (Symbolfoto)

- ① Optische Signalisierung
- ② Leseinheit
- ③ Stecker-Schnittstelle (EVVA-Logo)
- ④ Drücker mit Batteriefach

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

Der Xesar-Drücker signalisiert Ereignisse sowohl akustisch als auch optisch. Beachten Sie die Liste der unterschiedlichen akustischen und optischen Signale im Kapitel 2.2 Montage der Xesar-Zutrittskomponenten.

Der Xesar-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 Identmedium an der Leseinheit vorgehalten, wird der Außendrücker für 5 Sekunden mechatronisch eingekuppelt. Wird jetzt der Außendrücker betätigt, wird die Falle bzw. der Riegel – abhängig von der Schlosstypen – 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 Xesar-Drückers führen!

Der Xesar-Drücker kann bei leeren Batterien nur mit dem Notstromgerät (optionales Zubehör) betätigt werden.

Wenn Signal „Batterie schwach“ angezeigt wird, müssen die Batterien umgehend gewechselt werden. (Wenn das Signal „Batterie schwach“ 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 dazu das Kapitel 2.2 Montage der Xesar-Zutrittskomponenten.



Lassen Sie die Batterien nur von geschultem Fachpersonal wechseln!

Das Batteriefach befindet sich im Außendrucker des Xesar-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 Xesar-Drucker mit dem Xesar-Tablet synchronisiert werden!

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

- » Nehmen Sie das Drückerrohr des Außendruckers 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 dazu das Kapitel 2.2. Montage der Xesar-Systemkomponenten.

- » Setzen Sie das Drückerrohr wieder auf den Außendrucker.
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.

2.1.3 Xesar-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 Xesar-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 Xesar-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.



Abbildung 5: Xesar-Zylinder (Symbolfoto)

- 1 Optische Signalisierung
- 2 Leseinheit
- 3 Stecker-Schnittstelle (EVVA-Logo)

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

Der Xesar-Zylinder signalisiert Ereignisse sowohl akustisch als auch optisch. Beachten Sie die Liste der unterschiedlichen akustischen und optischen Signale im Kapitel 2.2 Montage der Xesar-Zutrittskomponenten.

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

Funktionsprinzip

Der elektronische Außenknopf des Xesar-Zylinders ist standardmäßig ausgekuppelt; bei Betätigung des Außenknopfs bleibt die Sperrnase ausgekuppelt und der Außenknopf dreht, ohne die Sperrnase mitzunehmen.

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

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

Wird ein berechtigtes Identmedium an der Leseinheit vorgehalten, wird der Außenknauf für 5 Sekunden mechatronisch eingekuppelt. Die Sperrnase des Xesar-Zylinders wird bei der Betätigung des Außenknaufts mitgenommen.

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

Der Xesar-Zylinder ist standardmäßig mit einer Rotationsbremse ausgestattet. Xesar-Zylinder mit Freilauffunktion (FZG) und Antipanic (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/>

Knauf-Achse fixieren

Alle Xesar-Zylinder in Europrofilausführung haben an der Stirnseite des Elektronikmoduls eine Servicebohrung. Um die Demontage des Zylinderknaufts 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 Xesar-Hangschloss

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



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



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



Abbildung 6: Xesar-Hangschloss (Symbolfoto)

- ❶ Optische Signalisierung
- ❷ Leseinheit
- ❸ Stecker-Schnittstelle (EVVA-Logo)

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

Das Xesar-Hangschloss signalisiert Ereignisse sowohl akustisch als auch optisch. Beachten Sie die Liste der unterschiedlichen akustischen und optischen Signale im Kapitel 2.2 Montage der Xesar-Zutrittskomponenten.

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

Funktionsprinzip

Der elektronische Außenknauf des Xesar-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 Leseinheit 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 Xesar-Hangschlosses, erfolgen. Die Sperrnase des Xesar-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/>

Zylinderwerkzeug

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



Abbildung 7: Zylinderwerkzeug (Symbolfoto)



Das Zylinderwerkzeug ist im Lieferumfang des Xesar-Zylinders nicht enthalten.

Option

Das Zylinderwerkzeug ist optional erhältlich:

Produktcode: E.ZU.PZ.ZW.V2

2.1.5 Xesar-Wandler

- Einsatz im Außen- und Innenbereich, Unter- oder Aufputz
- Geeignet für sicherheitsrelevante Bereiche
- Der Xesar-Wandler wird mit einer Steuereinheit mittels Anschlusskabel verbunden und von dieser stromversorgt.
- Über die mit dem Xesar-Wandler verbundene Steuereinheit können elektronische Verschlusselemente, wie z. B. Motorzylinder, Schwenktüren oder Schiebetüren angesteuert werden.

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service



Beachten Sie die mitgelieferten Sicherheitstexte, die zusätzlich wichtige Informationen zu Montage, Gebrauch und Wartung der Xesar-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).



Abbildung 8: Xesar-Wandleser (Symbolfoto)

- ❶ Optische Signalisierung
- ❷ Leseinheit und ON/OFF-Statusleuchte
- ❸ Stecker-Schnittstelle (EVVA-Logo)



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

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

Der Sensor der Leseinheit befindet sich hinter der Glasplatte des Xesar-Wandlers, 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 Xesar-Wandleser signalisiert Ereignisse sowohl akustisch als auch optisch. Beachten Sie die Liste der unterschiedlichen akustischen und optischen Signale im Kapitel 2.2 Montage der Xesar-Zutrittskomponenten.

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

Funktionsprinzip

Wird ein Identmedium an der Leseinheit vorgehalten, wird dieses Identmedium von der Steuereinheit, die mit dem Xesar-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 Xesar-Wandleser wird mittels Anschlussprint an die Verbindungsleitung der Steuereinheit angeschlossen.

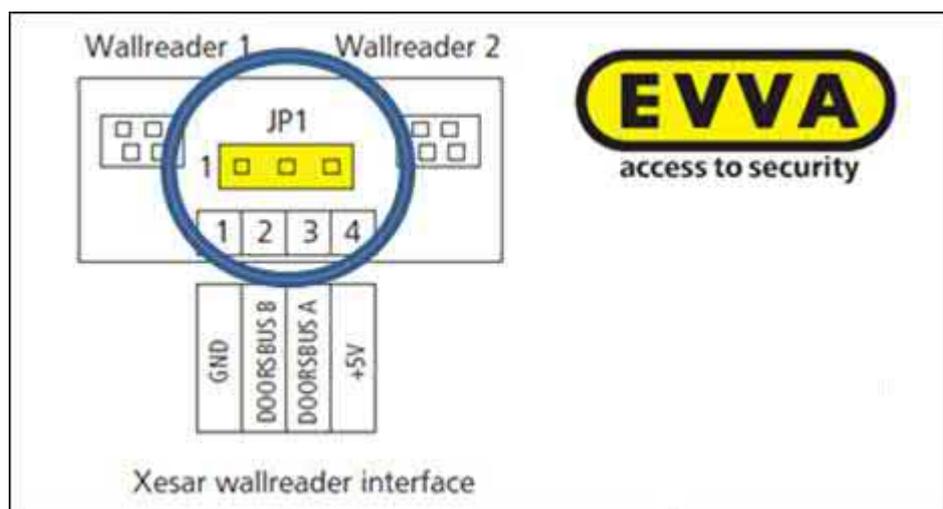


Abbildung 9: Anschlussprint für Xesar-Wandleser (Symbolfoto)



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

Steuereinheit



Abbildung 10: Steuereinheit (Symbolfoto)

Die Steuereinheit kann ausschließlich in Verbindung mit dem Xesar-Wandler betrieben werden. Es können zu 2 Xesar-Wandler angeschlossen werden. Die mit dem Xesar-Wandler 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.

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

Online-Steuereinheit

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

Die Online-Steuereinheit ist über den Ethernet Adapter via LAN mit dem Anlagenrechner verbunden. Unterbricht die LAN-Verbindung, agiert der Xesar-Wandler wie ein Offline-Wandler. 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 Xesar-Wandler 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 Xesar-Zutrittskomponenten



Lassen Sie die Xesar-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 Xesar-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 Xesar-Zutrittskomponenten stellt EVVA unter anderem folgende Hilfsmittel zur Verfügung:

- Sprachneutrale Montageanleitung
Die sprachneutrale Montageanleitung wird der entsprechenden Xesar-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/exdrz1/exdrz1-1/>

- Sprachneutrale Bohrschablone
Die sprachneutrale Bohrschablone wird der entsprechenden Xesar-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 Xesar-Beschläge und Xesar-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

Signalnummer	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 aktiver Dauerfreigabe	●●●●-●●●●	tttt—hhhh	
Signal 5	Dauerfreigabe Start	●●●●-●●●●	tttt—hhhh	
Signal 6	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 11	Kommunikationsvorgang mit PPD (Xesar)	●-●-●-●-●-●		
Signal 12	Kommunikation erfolgreich	●●●●●	hhhhh	
Signal 13	Kommunikation nicht erfolgreich	●●●●●	ttttt	
Signal 14	Medium berechtigt Offline	●●-●●-●●	mm-mm-mm	

Signalnummer	Ereignis	Optisches Signal	Akustisches Signal	Hinweis
Signal 15	Abgewiesenes Medium Offline	●●-●●-●●	mm-mm-mm	
Signal 16	Online Operation fehlgeschlagen	●●-●●-●●		

* 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 und Mini-Codierstation

Die Codierstation ist das Lese-/Schreibgerät für alle kontaktlosen Identmedien sowie für die kontaktbehaftete AdminCard, die zu den Systemkarten zählt (siehe Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**[AdminCard](#)).



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

Für die AdminCard steht ein eigener Karteneinschub-Slot am vorderen Ende der Codierstation zur Verfügung. Installieren Sie den zugehörigen Treiber und verbinden Sie die Codierstation mit der USB-Schnittstelle des Computers, auf dem die Xesar-Software installiert ist.

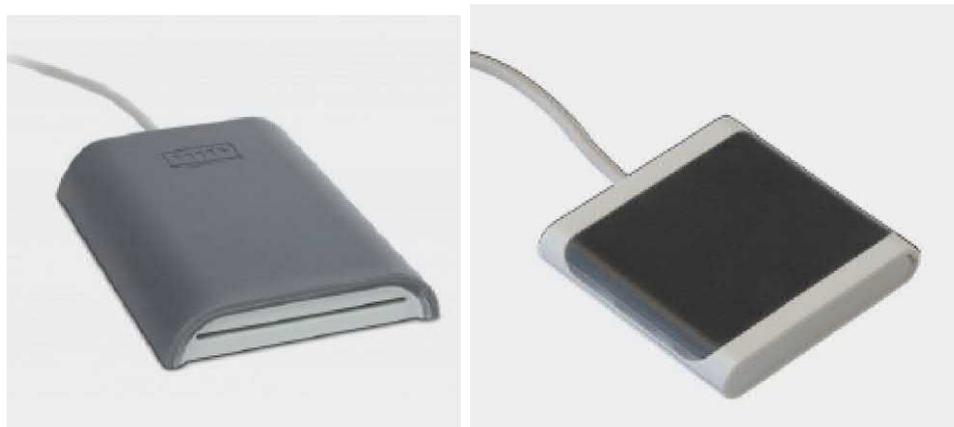


Abbildung 11: Codierstation und Mini-Codierstation (Symbolfotos)

Der Treiber für die Codierstation kann heruntergeladen werden:



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

Informationen zu weiteren Spezifikationen entnehmen Sie dem Datenblatt.

2.5 Xesar-Tablet

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



Abbildung 12: Xesar-Tablet (Symbolfoto)



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

Für das Xesar-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!

Zum Xesar-Tablet gehört ein spezielles Verbindungskabel von EVVA. Verwenden Sie dieses Verbindungskabel, um Ihre Xesar-Zutrittskomponenten mit dem Xesar-Tablet zu verbinden.

Das spezielle Verbindungskabel ist am EVVA-Logo, das sich auf dem USB-Stecker befindet, zu erkennen. Jede Xesar-Zutrittskomponente verfügt über eine eingebaute Stecker-Schnittstelle für die Synchronisation mit der Xesar-Software.

Die Stecker-Schnittstelle der Xesar-Zutrittskomponente befindet sich an der Vorderseite hinter dem EVVA-Logo. (Siehe Kapitel 2.1 Xesar-Zutrittskomponenten).



Synchronisieren Sie regelmäßig die Daten mit Ihren Xesar-Zutrittskomponenten.

Im Ereignisspeicher jeder Xesar-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 Xesar-Zutrittskomponenten mindestens einmal jährlich, um die Uhrzeit der Xesar-Zutrittskomponenten synchron zu halten.



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



Das Xesar-Tablet darf nicht für die Notstromversorgung der batteriebetriebenen Xesar-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 Xesar-Tablets mit der Xesar-Software werden alle Wartungsaufgaben und andere Aufgaben für die jeweilige Xesar-Zutrittskomponente auf das Programmiergerät geladen und protokolliert.

Verbinden Sie das Xesar-Tablet mit der Xesar-Zutrittskomponente. Der Datenaustausch wird mittels der Xesar-Tablet-App (Applikation) durchgeführt.

Xesar-Tablet-App

Die Xesar-Tablet-App ist auf dem Xesar-Tablet vorinstalliert.

Folgende Aktionen sind mit der Xesar-Tablet-App möglich:

- Xesar-Zutrittskomponenten „taufen“
(Initialisierung bei Inbetriebnahme)
- Geänderte Türparameter bei Xesar-Zutrittskomponenten synchronisieren
- Blackliste auf Xesar-Zutrittskomponenten übertragen
- Batteriezustand abfragen (auch bei Fremdanlagen)
- Aktuelle Firmware-Version abfragen (auch bei Fremdanlagen)
- Firmware-Update durchführen
Die Xesar-Zutrittskomponente im Batteriebetrieb wird während des Firmware-Updates durch das Xesar-Tablet mit Energie versorgt.
- Ereignisse von Xesar-Zutrittskomponenten auf Xesar-Tablet übertragen
- Xesar-Zutrittskomponente in Baustellenmodus zurücksetzen
- Die Uhrzeit der Xesar-Zutrittskomponente wird bei der Kommunikation mit dem Xesar-Tablet automatisch synchronisiert.


SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

2.6 Xesar-Notstromgerät

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



Sie benötigen zur Öffnung der notstromversorgten Xesar-Zutrittskomponente ein Identmedium mit MasterKey-Berechtigung, da bei zu langer Stromunterbrechung die Uhrzeit verloren geht. In diesem Fall können Identmedien mit Standard-Berechtigung die Xesar-Zutrittskomponente nicht mehr öffnen.

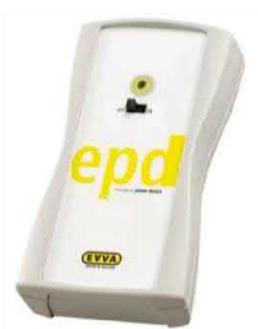


Abbildung 13: Notstromgerät (Symbolfoto)

- » Schließen Sie das Verbindungskabel des Notstromgeräts an der Stecker-Schnittstelle der entsprechenden Xesar-Zutrittskomponente an. Schalten Sie das Notstromgerät ein.

Eine weitere Interaktion am Notstromgerät selbst ist nicht erforderlich. Zur Bedienung der Xesar-Zutrittskomponente wird ein Medium mit gültiger Master Key-Berechtigung benötigt.

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



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



Das Notstromgerät ist optional erhältlich.

2.7 AdminCard

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

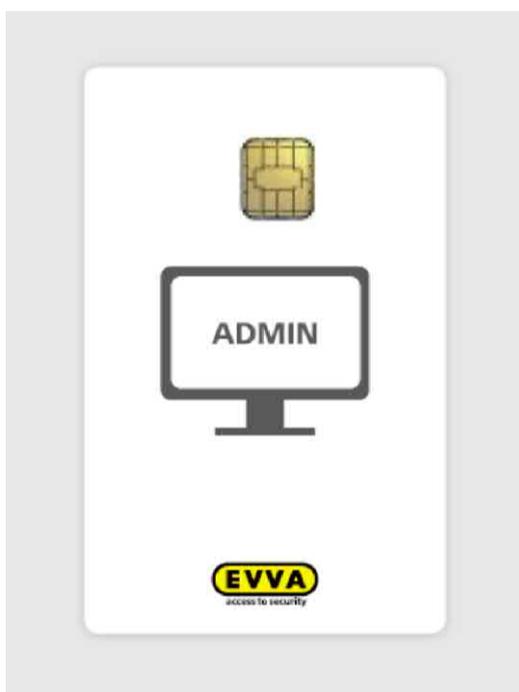


Abbildung 14: AdminCard (Symbolfoto)

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

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



Die AdminCard ist nicht übertragbar und kann daher nicht für andere Anlagen genutzt werden.

Bei Verlust oder Defekt kann die AdminCard ausgetauscht werden.

2.8 Xesar-Identmedien

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



Abbildung 15: Identmedien im Überblick

Identmedien sind berührungslose RFID¹-Chips, die auf MIFARE² DESFire EV1 mit einer Gesamtspeichergröße von 4 kB basieren.

- Mit Identmedien werden die Xesar-Zutrittskomponenten geöffnet. (Die Anlage darf sich dazu nicht im Baustellenmodus befinden. Im Baustellenmodus wurde die Xesar-Zutrittskomponente noch keiner Anlage elektronisch zugewiesen. Jede Xesar-Zutrittskomponente befindet sich im Auslieferungszustand im Baustellenmodus.)
- Mit der Codierstation werden Identmedien programmiert. Legen Sie dazu das Identmedium auf die betriebsbereite Codierstation und führen Sie die entsprechenden Interaktionen in der Xesar-Software durch.



Legen Sie immer nur ein Identmedium auf die Codierstation. Damit vermeiden Sie fehlerhafte Beschreibung der Identmedien.

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

Informationen zu weiteren Spezifikationen entnehmen Sie dem Datenblatt.



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

¹ RFID – radio-frequency identification

² MIFARE – Mikron Fare Collection System (kontaktlose Chipkartentechnik)



Anzahl der Berechtigungen pro Identmedium
(unabhängig von der Anzahl der zum Bereich
gehörenden Einbauorte)

max. 96 Türbereiche

Zusätzlich

32 Einbauorte

2.9 Construction-Card

Die Construction-Card ist das Baustellenmedium, das Xesar-Zutrittskomponenten im Baustellenmodus öffnen kann. (Im Baustellenmodus wurde die Xesar-Zutrittskomponente noch keiner Anlage elektronisch zugewiesen. Jede Xesar-Zutrittskomponente befindet sich im Auslieferungszustand im Baustellenmodus.) Zusätzlich ist mit der Construction-Card eine manuelle Dauerfreigabe möglich (siehe Kapitel 7.6 Zeitprofile).



Abbildung 16: Construction-Card (Symbolfoto)

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



Ihre Anlage kann im Baustellenmodus mit jeder Construction-Card bedient werden! Taufen Sie Ihre Xesar-Zutrittskomponenten daher ehestmöglich.



Für eine effiziente Inbetriebnahme der Anlage legen Sie zuerst Berechtigungsprofile sowie zugehörige Bereiche und Zeitprofile an. Konfigurieren Sie diese dann gleichzeitig mit der Taufe der Xesar-Zutrittskomponenten. (Siehe Kapitel 7 Inbetriebnahme der Xesar-Software.)

3 Systemanforderungen

Xesar kann sowohl als Einplatzanlage als auch als Mehrplatzanlage betrieben werden. Im Einplatzbetrieb verwaltet eine Person über einen PC die Xesar-Anlage. Im Mehrplatzbetrieb sind mehrere Clients mit dem Server verbunden und können unterschiedliche Aufgaben (z. B. Rezeption, Wartung) gleichzeitig durchführen.

Nachfolgend erhalten Sie die Systemanforderungen für Xesar 3.0.

3.1 Xesar 3.0 – Einplatzanlage

Wir empfehlen, vom Einsatz einer Einplatzanlage abzusehen, wenn ein 24/7-Dauerbetrieb oder der Einsatz von Online-Komponenten, wie z. B. den Xesar-Online Wandler gewünscht wird. Ist der Einplatz-PC nicht in Betrieb, ist der Xesar-Wandler im Offline-Modus und Identmedien werden nicht aktualisiert.

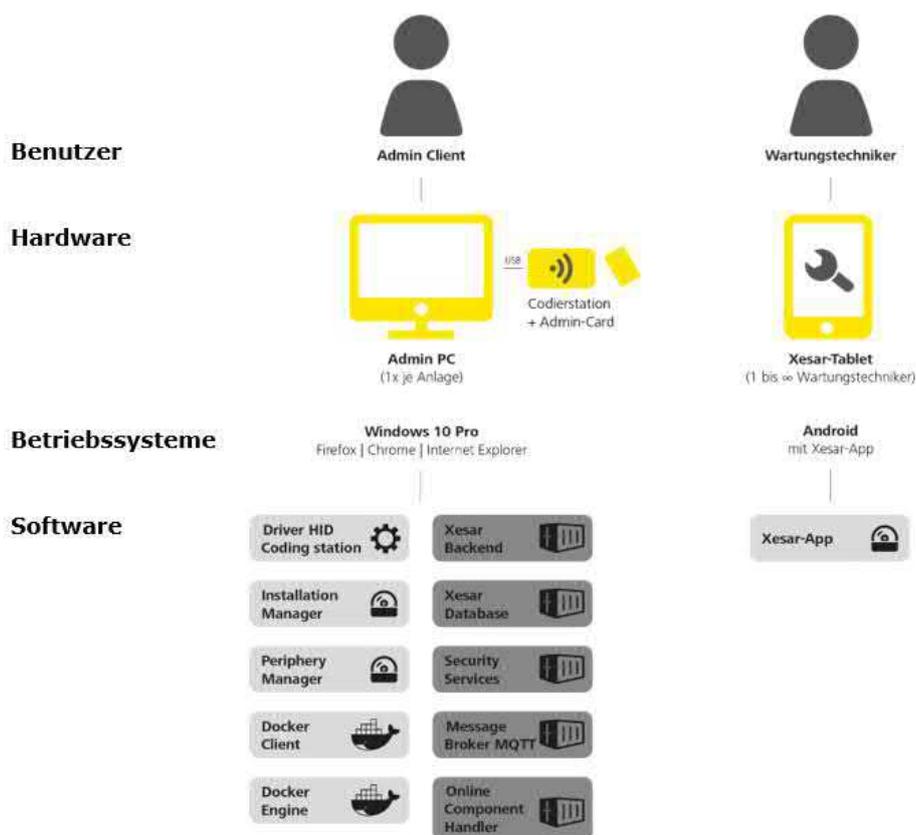


Abbildung 17: Übersicht Einplatzanlage

3.1.1 Systemanforderungen Einplatzanlage

	Mindestanforderung
Prozessor	x86-64 kompatibler Prozessor (CPU) 1-2-Core 2,4 GHz oder höher
	Hardware-Unterstützung für Virtualisierung
Arbeitsspeicher (RAM)	≥ 8 GB (mit OS)
Festplattenspeicher	≥ 60GB
Internet	Direkter Internetzugang ohne Proxy zur Freischaltung von KeyCredits und Lizenzen; Zugriff auf die durch EVVA besicherte authentische und nicht manipulierte Softwareauslieferung
Netzwerk (LAN, WLAN)	Lokales LAN mit Low Latency (Ping<10ms, Roundtrip <30ms); WLAN für die Xesar Tablet-Synchronisierung und Zugriff auf die bereitgestellten Services
	WLAN (Wireless): IEEE.802.11 g, n
Protokolle	IPv4 HTTP/HTTPS (mit TLS)
Software	Docker Client mit Unterstützung für API 1.24, Docker Compose 1.10.0+ (werden im Zuge der Docker-Installation am Admin-PC installiert)
	Docker Engine 1.12.0+ mit Unterstützung für API 1.24 (werden im Zuge der Docker-Installation am Admin-PC installiert)
Anschluss	1 × USB Host 2.0
Betriebssystem	Windows 10 Pro 64-Bit – Version 1511 (build 10586) oder höher
Browser	HTML5/CSS3 kompatibel, mit Javascript aktiviert
Peripheriegeräte	1 x Codierstation von EVVA mit Unterstützung für kontaktlose RFID Karten (Mifare Desfire EV1; ISO 14443) und mit Slot für AdminCard
	Keyboard und Maus
Monitor	Bildschirmauflösung 1024x768, empfohlen: 1920x1080

3.1.2 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 Xesar-Online Wandler – Server (Backend)

Service	Netzwerk	Default Port	Port Adresse	Protokoll	TLS	Nutzung	Nutzende Komponenten	Bereitstellende Komponente
Online Component-Handler	LAN/WLAN	9081	konfigurierbar	NWP	Ja	Kommunikation mit der Xesar-Software	Xesar-Online Wandler	Online-Component-Handler

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

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

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden
Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

3.2 Xesar 3.0 – Server Mehrplatzanlagen

Die Mehrplatzanlage besteht aus einem **Server**, einem **Admin-PC mit Codierstation und AdminCard** sowie gegebenenfalls weiteren **Client PCs mit oder ohne Codierstationen**.

Optional können auch **Mobile Geräte** über Browserzugang als Client ohne Codierstation verwendet werden. Das **Xesar-Tablet** wird als Wartungsgerät für die Anlagenverwaltung verwendet.



Beim Einsatz einer Mehrplatzanlage ist der Betrieb eines Servers im 24/7-Betrieb Voraussetzung!

Die folgende Übersicht enthält verschiedene Einsatzvarianten.

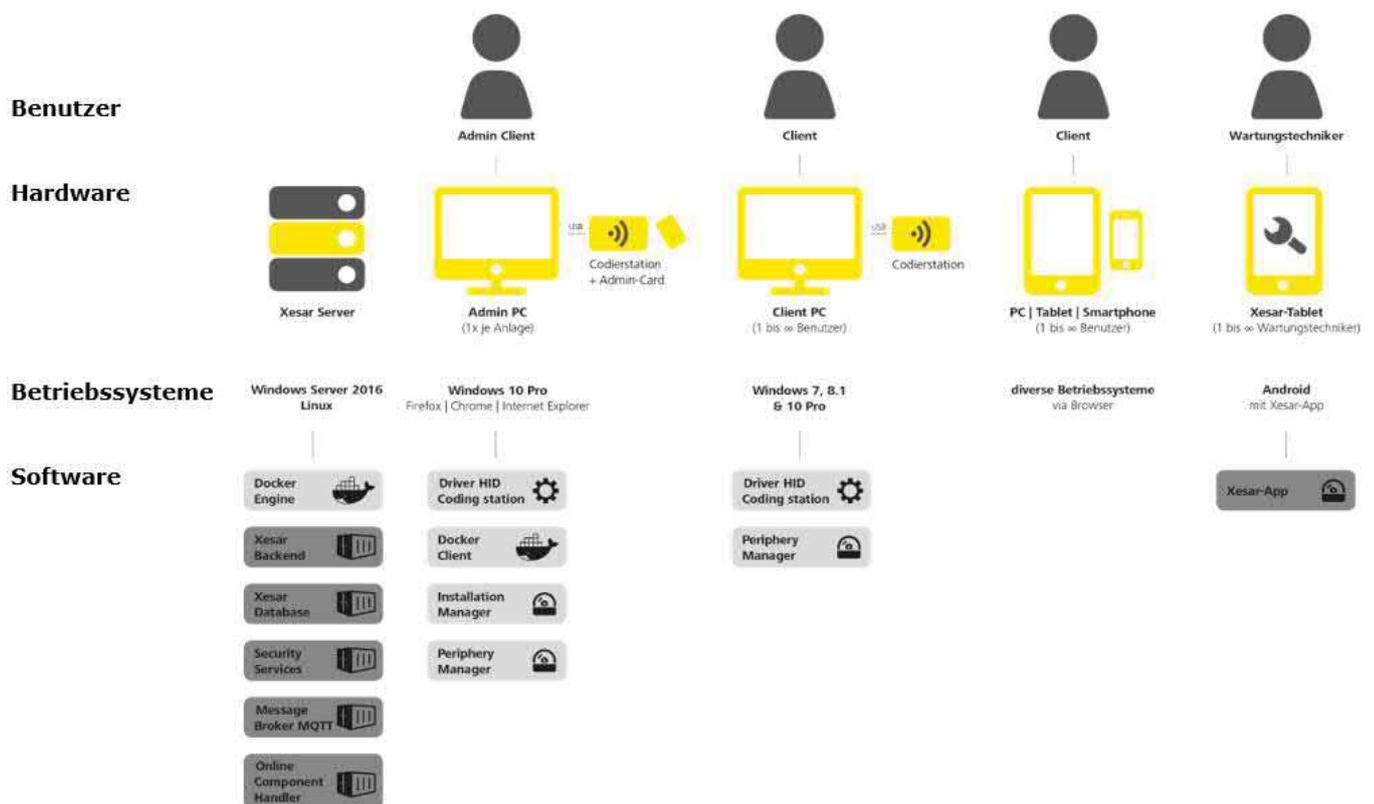


Abbildung 18: Übersicht Mehrplatzanlage

3.2.1 Systemanforderungen Server

	Mindestanforderung
Prozessor	x86-64 kompatibler Prozessor (CPU) mindestens Quad-Core \geq 1,5-2,3 GHz
	Hardware-Unterstützung für Virtualisierung
Arbeitsspeicher (RAM)	\geq 4 GB (mit OS; min. 2GB für den Server Software Stack)
Festplattenspeicher, SSD empfohlen	\geq 40GB (Systemgröße und geplante Laufzeit bei der Dimensionierung beachten)
Internet	Direkter Internetzugang ohne Proxy zur Freischaltung von KeyCredits und Lizenzen den Zugriff auf die durch EVVA besicherte authentische und nicht manipulierte Softwareauslieferung
Netzwerk (LAN, WLAN)	Lokales LAN mit Low Latency (Ping<10ms, Roundtrip <30ms)
	WLAN zur Xesar-Tablet-Synchronisation mit Server
	Zugriffsmöglichkeit aus dem lokalen LAN auf den Server für bereitgestellte Services
Software	Docker Engine 1.12.0+ mit Unterstützung für API 1.24 (werden im Zuge der Docker-Installation installiert)

Service Katalog siehe Kapitel 3.4 Server-Kommunikation:

- Server – Admin PC
- Server – Client PC
- Server – Online Wandler

3.2.2 Getestete Betriebssysteme

OS	OS Typ	Version	Virtualisierung möglich
Ubuntu	Linux	14.04 (Trusty, LTS) 16.04 (Xenial, LTS) 18.04.1 / 18.04.2 LTS	Ja
Windows Server	Windows	2016 Datacenter 2016 Standard	Nein

OS	OS Typ	Version	Virtualisierung möglich
DSM ³	Linux	6.1	Nein
		6.2	
Photon OS ⁴	Linux	2.0	Ja



Xesar muss im Betrieb bei der Kommunikation mit den Online-Komponenten Echtzeitanforderungen erfüllen. Wenn der Windows Server 2016 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.

3.2.3 Nicht getestete Betriebssysteme

OS	OS Typ	Version	Virtualisierung möglich
Cent OS	Linux	7	Ja
Debian	Linux	9 (Stretch)	Ja
		8 (Jessie, LTS)	
Fedora	Linux	26, 27	Ja



Aufgrund der Vielzahl möglicher Betriebssysteme und der fortlaufenden Entwicklungen am IT-Markt können nicht alle Varianten im Vorfeld auf Kompatibilität von EVVA getestet werden.

Bei Bedarf fordern Sie die aktuelle Kompatibilitätsliste bei Ihrem EVVA Partner oder den Technischen Büros von EVVA an.

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

³ Betriebssystem für Synology NAS; Verifizierung erfolgt auf DS916+

⁴ Container optimiertes Betriebssystem von VMware empfohlen für VMware vSphere ESXi 6.x

3.2.4 Systemanforderungen Admin-PC mit Codierstation und AdminCard

Für den Betrieb des Xesar-Installation Managers (Anlagenverwaltungssoftware) müssen folgende Mindestanforderungen erfüllt sein:

	Mindestanforderung
Prozessor	x86-64 kompatibler Prozessor (CPU) 1-2-Core 2,4 GHz oder höher
	Hardware-Unterstützung für Virtualisierung
Arbeitsspeicher (RAM)	≥ 4 GB (mit OS; min. 1GB für die Applikationen: Xesar-Installation Manager und Xesar-Periphery Manager)
Festplattenspeicher	≥ 5GB
Internet	Direkter Internetzugang ohne Proxy zur Freischaltung von KeyCredits und Lizenzen den Zugriff auf die durch EVVA besicherte authentische und nicht manipulierte Softwareauslieferung
Netzwerk (LAN, WLAN)	Lokales LAN für den Zugriff auf die vom Xesar 3.0 Server bereitgestellten Services
Software	Docker Client mit Unterstützung für API 1.24, Docker Compose 1.10.0+ (werden im Zuge der Docker-Installation am Admin-PC installiert)
Anschluss	1 × USB Host 2.0
Betriebssystem	Windows 10 Pro 64-Bit – Version 1511 (build 10586) oder höher
Browser	HTML5/CSS3 kompatibel, mit Javascript aktiviert
Peripheriegeräte	1 x Codierstation von EVVA mit Unterstützung für kontaktlose RFID Karten (Mifare Desfire EV1; ISO 14443) und mit Slot für AdminCard
	Keyboard und Maus
	Monitor: Bildschirmauflösung 1024x768, empfohlen: 1920x1080

Service Katalog siehe Kapitel 3.4 Server-Kommunikation:

- Admin-PC – Server

3.2.5 PC Betriebssysteme:

OS	Version	Browser	EVVA- verifiziert	EVVA Codier- station
Windows	10 Pro (V 1511 – build 10586)	Firefox ab Version 47 Chrome ab Version 48 Internet Explorer ab 11	Ja	Ja

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

- Betrieb des Xesar-Installation Managers auf einer virtuellen Maschine am Server (AdminCard wird über Client-PC verbunden)
- Betrieb des Xesar-Installation Managers auf anderen Windows Betriebssystemen, wie Windows 7, 8.x, Server 2012 R2 und Server 2016 Datacenter
- Betrieb des Xesar-Periphery Managers auf anderen Windows Betriebssystemen, wie Windows Server 2012 R2 und Server 2016 Datacenter
- Betrieb des Xesar-Periphery Managers auf anderen Betriebssystemen (nur auf Anfrage)
- Einsatz anderer HTML5/CSS3 kompatibler Browser

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

3.2.6 Systemanforderung Client-PC mit Codierstation ohne AdminCard

Für den Betrieb eines Client-PC **mit** Codierstation im Mehrplatzsystem müssen folgende Mindestanforderungen erfüllt sein:

	Mindestanforderung
Prozessor	x86-64 kompatibler Prozessor (CPU) 1-2-Core 2,4 GHz oder höher
Arbeitsspeicher (RAM)	≥ 4 GB (mit OS; min. 512MB für die Xesar-Peripherie-Manager Applikation, 1-2 GB für einen unterstützten Browser)
Festplattenspeicher	≥ 2GB
Netzwerk (LAN, WLAN)	Lokales LAN für den Zugriff auf die vom Xesar 3.0 Server bereitgestellten Services
Anschluss	1 × USB Host 2.0
Browser	HTML5/CSS3 kompatibel, mit Javascript aktiviert
Peripheriegeräte	1 x Codierstation von EVVA mit Unterstützung für kontaktlose RFID Karten (Mifare Desfire EV1; ISO 14443)
	Keyboard und Maus
Monitor	Bildschirmauflösung 1024x768, empfohlen: 1920x1080

Service Katalog Server und Arbeitsplätze im Mehrplatzsystem

Siehe Anlage: 3.5 Kommunikation Client PC - Server (Backend)

- Client-PC – Server

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

3.2.7 Betriebssysteme:

OS	Version	Browser	EVVA-verifiziert	EVVA Codierstation
Windows	7 Pro, 64-Bit		Ja	Ja
Windows	8.1 Pro, 64-Bit	Firefox ab Version 47 Chrome ab Version 48 Internet Explorer ab 11	Ja	Ja
Windows	10 Pro, 64-Bit		Ja	Ja

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

- Betrieb des Xesar-Periphery Managers auf anderen Windows Betriebssystemen, wie Windows Server 2012 R2 und Server 2016 Datacenter
- Betrieb des Xesar-Periphery Managers auf anderen Betriebssystemen (nur auf Anfrage)
- Einsatz anderer HTML5/CSS3 kompatibler Browser

3.2.8 Systemanforderungen Client PC ohne Codierstation (PC/Tablet/Smartphone)

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

	Mindestanforderung
Prozessor	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	≥ 2GB
Netzwerk (LAN, WLAN)	Lokales LAN für den Zugriff auf die vom Xesar 3.0 Server bereitgestellten Web-Services

	Mindestanforderung
Browser	HTML5/CSS3 kompatibel, mit Javascript aktiviert
	Keyboard und Maus
Monitor	Bildschirmauflösung 1024x768, empfohlen: 1920x1080

Service Katalog Server und Arbeitsplätze im Mehrplatzsystem

Siehe Anlage: 3.5 Kommunikation Client PC - Server (Backend)

3.2.9 Betriebssysteme:

OS	Version	Browser	EVVA-getestet
Windows	7 Pro		Ja
Windows	8.1 Pro	Firefox ab Version 47 Chrome ab Version 48 Internet Explorer ab 11	Ja
Windows	10 Pro		Ja

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

- Betrieb auf anderen Windows Betriebssystemen, wie Windows Server 2012 R2 und Server 2016 Datacenter
- Vergleichbare Browser auf anderen Betriebssystemen (nur auf Anfrage)
- Einsatz anderer HTML5/CSS3 kompatibler Browser

3.2.10 Systemanforderungen Netzwerk (Lokales Netzwerk und Internet)

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

	Mindestanforderung
Lokales Netzwerk	Fast Ethernet 100Base-TX 100Mbit, Standard MTU (1500 Bytes) oder besser
	Low-Latency zwischen den verbundenen Bausteinen (Ping<10ms, Round-trip <30ms)
	WLAN (Wireless): IEEE.802.11 g, n
Protokolle	IPv4
	HTTP/HTTPS (mit TLS)
	MQTT (mit TLS)
	EVVA NWP (mit Transportsicherung; Online Wandler)

3.2.11 Bereitgestellte Services im Internet

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



■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

3.2.12 Bereitgestellte Services im lokalen Netzwerk

Service	URL: Port	Was	Port-konfigurierbar
Docker Engine	<u><a href="tcp://<IP Installation>:2376">tcp://<IP Installation>:2376</u>	Host	Ja
Sicherheitservice	<u><a href="https://<IP Installation>:8200">https://<IP Installation>:8200</u>	Installation	Ja
Message Broker	<u><a href="mqttp://<IP Installation>:1883">mqttp://<IP Installation>:1883</u>	Peripherie, Schnittstelle	Ja
Verwaltung	<u><a href="https://<IP Installation>:8080">https://<IP Installation>:8080</u>	Betrieb	Ja
Online Komponenten Handler	<u><a href="tcp://<IP Installation>:9085">tcp://<IP Installation>:9085</u>	Betrieb	Ja

3.3 Anhang

Verteilungssicht

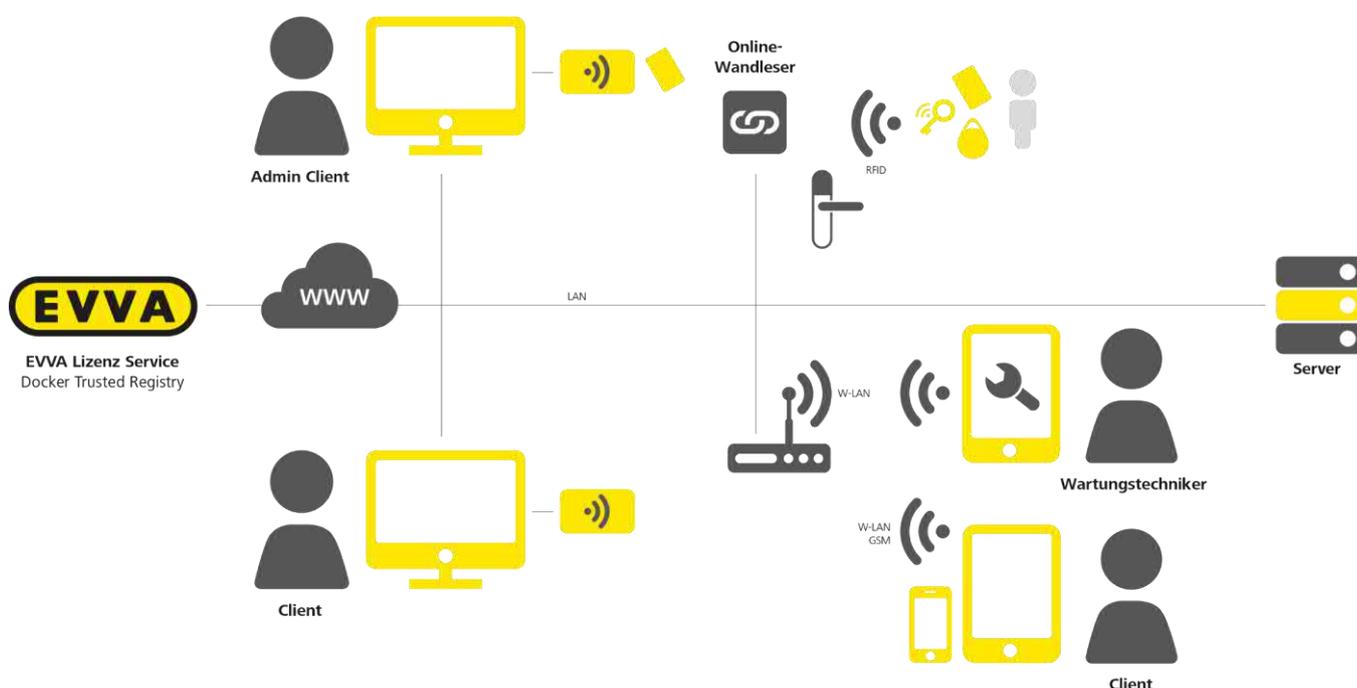


Abbildung 19: Verteilungssicht

3.4 Service Katalog: 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/AdminCard und Laden von Key-Credit Codes	Xesar-Installation Manager	Lizenzservice
5	AdminCard Terminal	USB	Fix	–	ISO 14443	–	Lesen und schreiben von Identmedien	Installations-Verwaltung über den Peripherie-Manager (nur Proxy)	Codierstation
6	Installations-Verwaltung Frontend Web Service	LAN/WLAN	8080	Konfigurierbar	HTTPS	Ja	Web Service und Auslieferung der Web Applikation für den Browser	Browser	
7	Online Component-Handler	LAN/WLAN	9081	Konfigurierbar	NWP	Ja	Kommunikation mit der Xesar-Software	Xesar-Online-Wandler	Online-Component-Handler

Anwendungen

Admin PC mit Xesar-Installation Manager:

- 1: Anlagen Start
- 2: Anlagen Stop
- 3: Anlagen Update
- 4: Lizenzservice (KeyCredits aufladen)
- 5: mit Codierstation für AdminCard

Client PC:

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

Online Wandlerer:

- 7: Online Wandlerer Kommunikation

Server und Arbeitsplätze im Mehrplatzsystem

3.5 Service Katalog: Kommunikation Client-PC – Server (Backend)

Service	Netzwerk	Default Port	Port Adresse	Protokoll	TLS	Nutzung	Nutzende Komponenten
Installations-Verwaltung Frontend Web Service	LAN/WLAN	8080	konfigurierbar	HTTP	Ja	Web Service und Auslieferung der Web Applikation für den Browser	Browser
Message Broker*	LAN/WLAN	1883	konfigurierbar	MQTT	Ja	Asynchrone Xesar System Schnittstelle	Peripherie-Manager
Codierstation*	USB	fix	–	ISO 14443	–	Lesen und schreiben von Identmedien	Installations-Verwaltung über den Peripherie-Manager (nur Proxy)

*Nur bei Client-PC mit Codierstation

Service Katalog: Xesar-Online Wandlerer Anbindung
an eine Xesar-3 Anlage

3.6 Kommunikation Online Wandlerer – Server (Backend)

Service	Netzwerk	Default Port	Port Adresse	Protokoll	TLS	Nutzung	Nutzende Komponenten	Bereitstellende Komponente
Online Component-Handler	LAN/ WLAN	9081	konfigurierbar	NWP	Ja	Kommunikation mit der Xesar-Software	Xesar-Online Wandlerer	Online-Component-Handler

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden
Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

4 Anlageninstallation Upgrade und Updates

4.1 Upgrade von Xesar 2.2 auf Xesar 3.0

Bei einem Upgrade von Xesar 2.2 auf Xesar 3.0 sind folgende Maßnahmen bzw. Konsequenzen zu berücksichtigen:



Xesar-Software

Betriebssystem des PCs: Windows 10 Pro



Xesar-Tablet

WLAN wird vorausgesetzt



Xesar-Zutrittskomponenten

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



Xesar-Wandler

Prozedere bei Konstellation „Steuereinheit und zwei Xesar-Wandler“:

- » Xesar-Wandler aus der Anlage ausbauen und in den Baustellenmodus versetzen
- » Nach der Installation von Xesar 3.0 die Xesar-Wandler in die Anlage einbringen.



AdminCard

Als AdminCard muss die X2.2-Karte verwendet werden



Identmedien

Keine Änderungen nötig



KeyCredits

Guthaben der Stück-KeyCredits werden übernommen.

KeyCredits Unlimited gehen verloren.

4.1.1 Upgrade-Kompatibilität von Xesar



Ein Upgrade auf Xesar 3.0 ist nur von Anlagen mit Xesar 2.2 möglich.
Gilt für Firmware und Software.

Soll / Ist	X1.0	X1.1	X2.0	X2.1	X2.2	X3.0
X1.0						
X1.1	•					
X2.0		•				
X2.1		•	•			
X2.2		•	•	•		
X3.0					•	

Folgende Xesar-Tablets werden mit Xesar 3.0 unterstützt:

- Xesar-Tablet V3 (EVVA – Ares F716XM)
- Xesar-Tablet V2 (Acer Iconia One 7 (B1-770 und B-730HD))

4.1.2 Anleitung für Upgrade Xesar 2.2 auf Xesar 3.0

Für das Upgrade Xesar 2.2 auf Xesar 3.0 beachten Sie folgende Punkte

- Ereignisprotokolldaten können nicht von Xesar 2.2 in Xesar 3.0 übernommen bzw. importiert werden.

Kopieren Sie die Ansicht der Ereignisprotokolle unter Xesar 2.2, bevor Sie die Anlage auf Xesar 3.0 upgraden.

- Für den Xesar 2.2 Datenimport muss die persönliche Firewall das Mounten grundsätzlich zulassen bzw. darf die benötigten Ports nicht blockieren.
- Auf Ihrem Xesar-Tablet muss die bestehende Xesar-App deinstalliert und die neue Xesar 3.0-App installiert werden (siehe Kapitel 5.7 Manuelle Deinstallation und Installation der Xesar-App).
- Die aktuelle Firmware der Xesar-Zutrittskomponenten für Xesar 3.0 wird mit dem Xesar-Tablet und der aktuellen Xesar-App auf die Komponenten übertragen.
- Die bereits vorhandenen Identmedien können weiterverwendet werden. Sie müssen dazu auf der Codierstation oder einem Xesar-Online Wandler aktualisiert werden.
- Vor dem Import einer Xesar 2.2-Anlage in eine Xesar 3.0-Anlage muss das Laufwerk C für Docker freigeschaltet werden.
- Eine Xesar-2.2.x-Anlage kann nur in der gleichen Zeitzone importiert und betrieben werden.
- Die vorhandene AdminCard Ihrer Xesar 2.2-Anlage wird weiterverwendet.
- Stück-KeyCredits können weiterverwendet werden.
- KeyCredit Unlimited können bei Xesar 3.0 nicht weiterverwendet werden und **verfallen!**



Verwenden Sie KeyCredit Xesar Lifetime für die unbeschränkte Verwendung mit nur einmaliger Bezahlung!

- Die Xesar Lifetime Lizenz darf erst nach erfolgtem Update auf Xesar 3.0 eingelöst werden. Die **Lizenz NICHT in Xesar 2.2** (also vor dem Export/Import nach Xesar 3.0!) einlösen.
- **Zwei Xesar-Wandler mit einer Steuereinheit CU:**
Verwenden Sie in Ihrer Xesar 2.2-Anlage die Konstellation „Zwei Xesar-Wandler mit einer Steuereinheit“, müssen diese Wandler **vor** dem Upgrade auf Xesar 3.0 aus der Anlage ausgebaut und in den Baustellenmodus gebracht werden. Nach dem Upgrade auf Xesar 3.0 bauen Sie die beiden Xesar-Wandler wieder in die Anlage ein.
- Wird eine Xesar 2.2-Anlage mit einem **Berechtigungsprofil „Feuerwehr“** in Xesar 3.0 importiert, kann es vorkommen, dass in Xesar 3.0 ein weiteres

Feuerwehreberechtigungsprofil erzeugt wird. In diesem Fall muss ein Feuerwehrprofil manuell entfernt werden.

- Nachdem eine Xesar 2.2-Anlage nach Xesar 3.0 importiert wurde, dürfen die EVVA-Komponenten nicht mehr mit der Xesar 2.2-Anlage synchronisiert werden. Nach erfolgreichem Import darf **nur mehr mit Xesar 3.0** weitergearbeitet werden.

Für das Upgrade Xesar 2.2 auf Xesar 3.0 gehen Sie wie folgt vor:

- » Stecken Sie Ihre AdminCard in den Slot der Codierstation.
- » Laden Sie die Daten aus Ihrer Xesar 2.2-Anlage (siehe Kapitel 7.1 Xesar-Installation Manager – AdminCard laden)
- » Wählen Sie „Hinzufügen einer neuen Anlage“ und importieren Sie Ihre Xesar 2.2 Datenbankdatei.



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

4.2 Vorbereitung des PCs für die Xesar 3.0-Installation

Vor Start der Installation von Xesar 3.0 müssen auf dem Anlagen-PC (Windows 10 Pro) Docker und der Treiber für die Codierstation installiert werden.

4.2.1 Docker Installation

Docker ist eine Open-Source-Software zur Isolierung von Anwendungen mit Containervirtualisierung. Zunächst muss Docker auf Ihrem PC installiert werden.



Docker CE for Windows kann nur auf PCs mit Windows 10 Pro ab Version 1511 (build 10586) installiert werden. Führen Sie ein Windows 10 Pro-Update durch, wenn die notwendige Windows 10 Pro Version nicht installiert ist.

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden
Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

4.2.2 Download Docker



Die **aktuell getestete und freigegebene Docker-Version** ist Docker Community Edition 18.06.1-ce-win73 2018-08-29.

Neuere Versionen erfragen sie bitte **vor** der Installation bei ihrem EVVA Technischen Büro.

Bei einer Neuinstallation von Docker (Docker deinstallieren und danach wieder installieren) gehen alle Anlagen-Daten verloren.

Daher müssen **bevor** Docker deinstalliert wird, alle Container gesichert werden. Dies kann ab Version Xesar 3.0 SP1 mit der **manuellen oder automatischen Backup-Funktion im Xesar-Installation Manager** durchgeführt werden.

Vor einem Docker Update muss die Xesar-Anlage im Xesar-Installation Manager gestoppt werden.

Nach dem Import einer Xesar 2.2-Anlage müssen die Identmedien aktualisiert werden.

» Docker auf Ihren Rechner laden



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

4.2.3 Docker installieren

Nach dem Download öffnet sich automatisch der Installer.

» **1. Schritt**

Docker herunterladen.



Abbildung 20: Installation Docker

Falls eine Warnmeldung von Windows angezeigt wird, klicken Sie auf **Ja**.

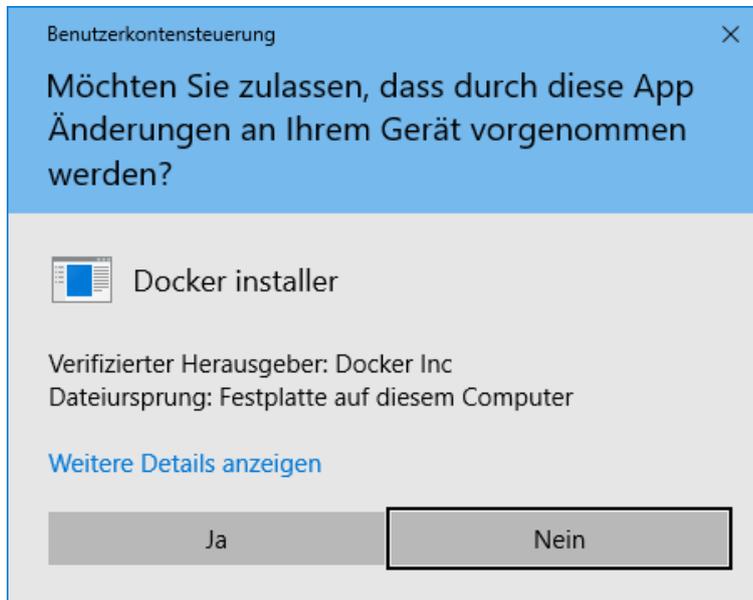


Abbildung 21: Installation Docker - Sicherheitshinweis

» 2. Schritt:

Docker starten

- In der Windows-Taskleiste öffnet sich automatisch die Statusmeldung **Docker is starting....**
- Wenn sich die Statusmeldung nicht öffnet, klicken Sie mit Doppelklick auf die Verknüpfung **Docker for Windows** auf ihrem Desktop.



Der Start kann einige Minuten dauern



Abbildung 22: Docker starten



Abbildung 23: Docker Startfortschritt

» 3. Schritt:

Docker ist now up and running!

Wenn Docker gestartet wurde öffnet sich ein Statusfenster mit der Meldung

Docker is now up and running!

Das Statusfenster schließt sich automatisch.

Rechtsklick auf das Docker-Symbol, um die Einstellungen zu öffnen.



Abbildung 24: Docker Statusfensterzeit

» 4. Schritt:

Klicken Sie auf **Settings**

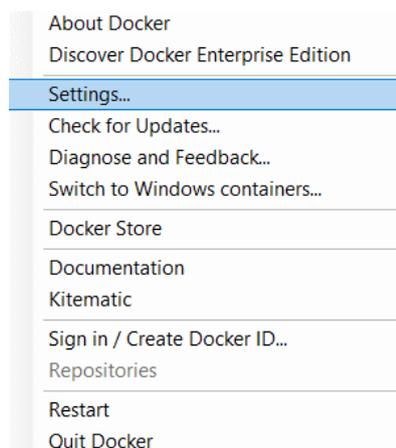


Abbildung 25: Docker Statusfensterzeit

» **5. Schritt:**

Kontrollieren Sie die Settings: Die Einstellungen für ❶, ❷ und ❸ dürfen **NICHT** gesetzt sein:

- ❶ Start Docker when you log in
- ❷ Automatically check for updates
- ❸ Send usage statistics

Beenden Sie die Einstellungen von Docker ❹ x.

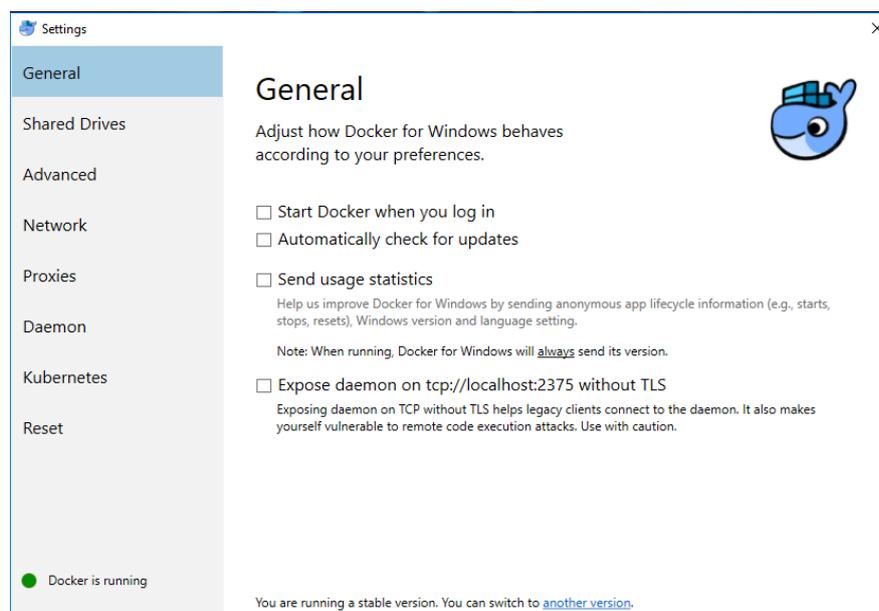


Abbildung 26: Docker Einstellungen-Auswahl (Settings)



Für die Verwendung von Docker muss der PC **Hyper-V Virtualisierung** unterstützen.
Hyper-V Virtualisierung muss aktiviert sein!

Die Zertifikate für die Verbindungen zwischen den Containern / Diensten laufen ein Jahr. Wenn eine Anlage eine überdurchschnittlich lange Zeit (> 1 Jahr) über den Xesar-Installation Manager nicht gestartet wird, laufen die Zertifikate ab. Dadurch kann es zu Fehlfunktionen und Fehlermeldungen in der Xesar-Software kommen. Starten Sie den Xesar-Installation Manager, damit sich die Zertifikate beim erstmaligen Starten erneuern. (Der Zustand regeneriert sich nach wenigen Minuten von selbst.)

Docker ist nun auf ihrem PC installiert!
Installieren Sie als nächstes den Treiber für die Codierstation!



Falls Hyper-V nicht aktiviert ist, geben Sie in der Kommandozeile „Windows Features“ ein. Klicken Sie auf Windows-Features aktivieren oder deaktivieren.



Bei einer Neuinstallation von Docker (Docker deinstallieren und wieder installieren) gehen alle Anlagen-Daten verloren.

Sichern Sie alle Anlagen-Daten, bevor Sie Docker deinstallieren. (Siehe 6 Kapitel Sicherung der Xesar-Anlagendaten im Xesar-Installation Manager).



Abbildung 27: Windows Features

- » Scrollen Sie nach unten bis **Hyper-V** und aktivieren Sie es. Klicken Sie anschließend auf „OK“.


SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

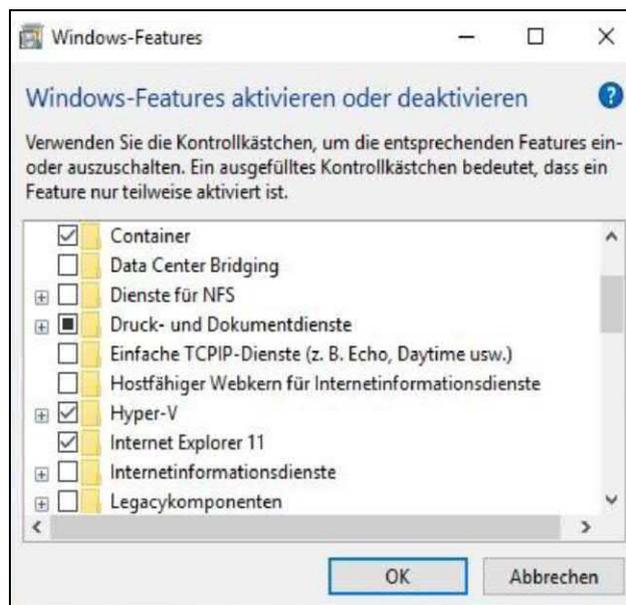


Abbildung 28: Windows Features

4.2.4 Installation des Treibers für die Codierstation



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

Falls die Version HID Omnikey 5422 der Codierstation haben, ist keine Treiberinstallation notwendig. (In diesem Fall direkt mit Kapitel 5 Xesar 3.0 Programme fortfahren.)

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

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

4.2.5 Automatische Treibersuche über Windows

Zur Treiberinstallation der Codierstation verwenden Sie bitte den Windows Gerätemanager.

» 1. Schritt:

Stecken Sie Ihre Codierstation ohne AdminCard an den USB Anschluss Ihres PC an!

» **2. Schritt:**

Öffnen Sie den „Geräte-Manager“ über die Windows Suchleiste.

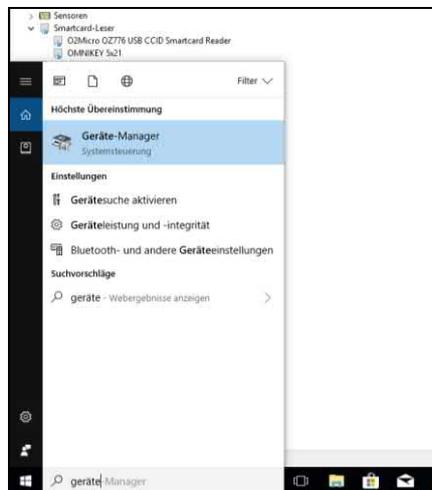


Abbildung 29: Windows Geräte-Manager

» **3. Schritt:**

➊ 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.

➋ Rechtsklick auf den Eintrag **Microsoft...** und wählen Sie **Treiber aktualisieren**.

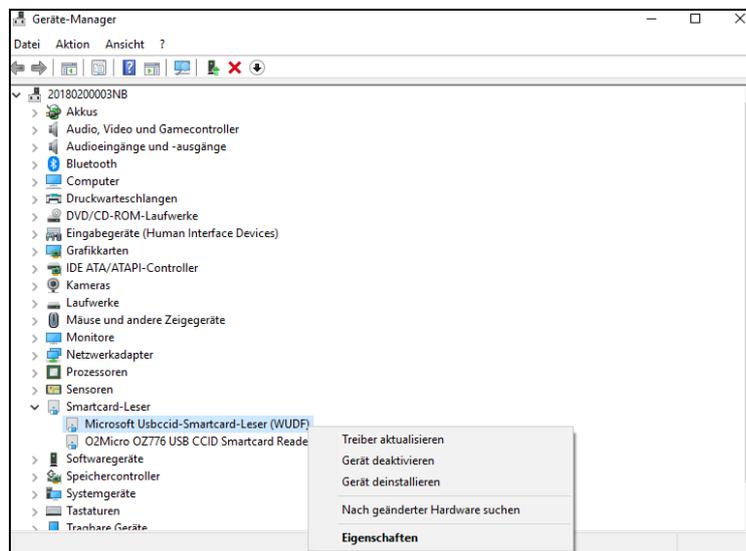


Abbildung 30: Microsoft Treiber aktualisieren

» **4. Schritt:**

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

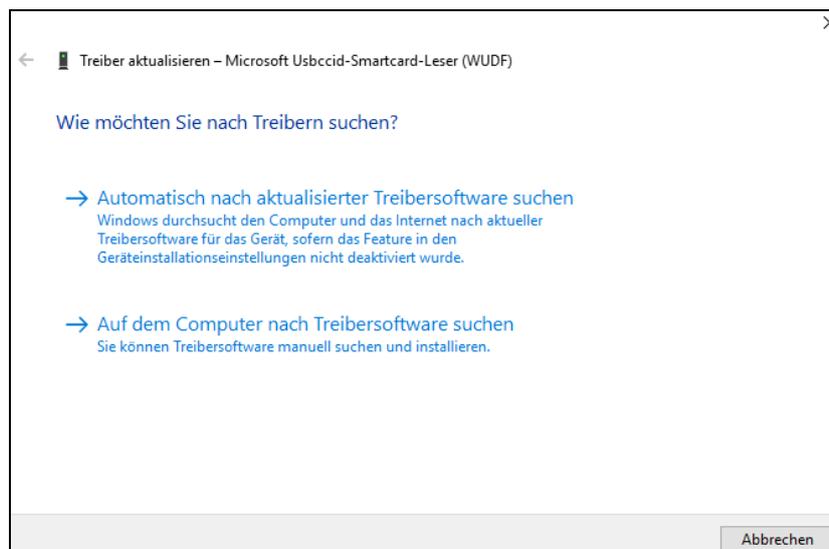


Abbildung 31: Treibersuche

» **5. Schritt:**

Der Treiber wird nun automatisch heruntergeladen und installiert!

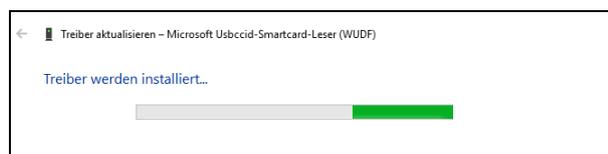


Abbildung 32: Codierstation - Automatische Treiberinstallation

» **6. Schritt:**

Der Treiber wurde installiert. Klicken Sie auf **Schließen**.

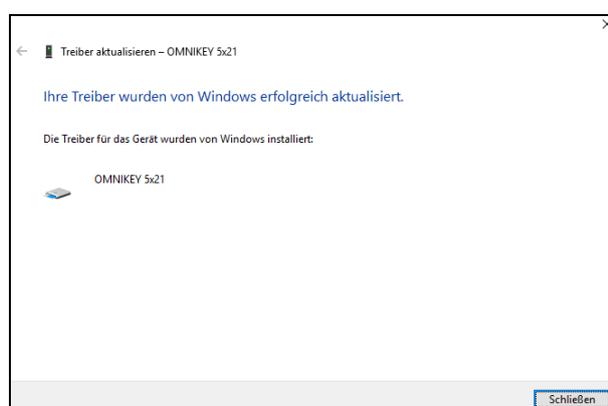


Abbildung 33: Codierstation- Erfolgreiche Treiberinstallation

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

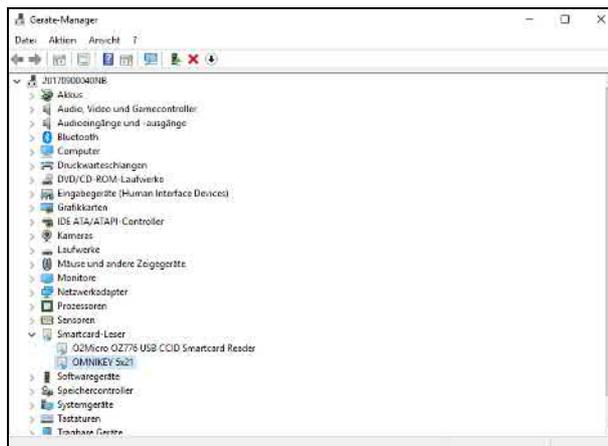


Abbildung 34: Anzeige der Codierstation im Geräte-Manager

Die Installation des Treibers für die Codierstation ist damit abgeschlossen. Als nächsten Schritt mit Kapitel 5 Xesar 3.0 Programme fortfahren

4.2.6 Manuelle Treibersuche auf der Homepage des Herstellers

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.de/drivers>



Abbildung 35: Treibersuche (Produkt) bei HID Global

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

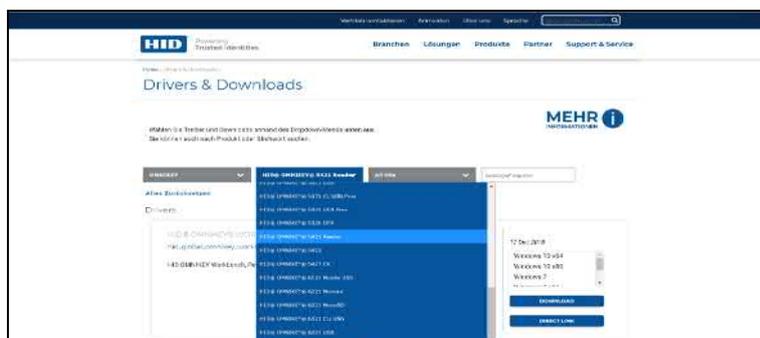


Abbildung 36: Treibersuche (Modell) bei HID Global

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



Abbildung 37: Treibersuche (Betriebssystem) bei HID Global

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**.



Abbildung 38: Treibersuche (Betriebssystem) bei HID Global

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.


SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

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

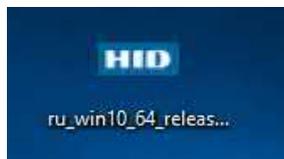


Abbildung 39: Anwendung Treiberinstallation für Codierstation

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

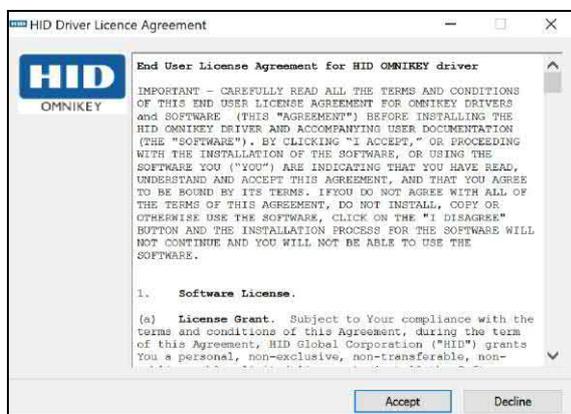


Abbildung 40: Treiberinstallation für Codierstation

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

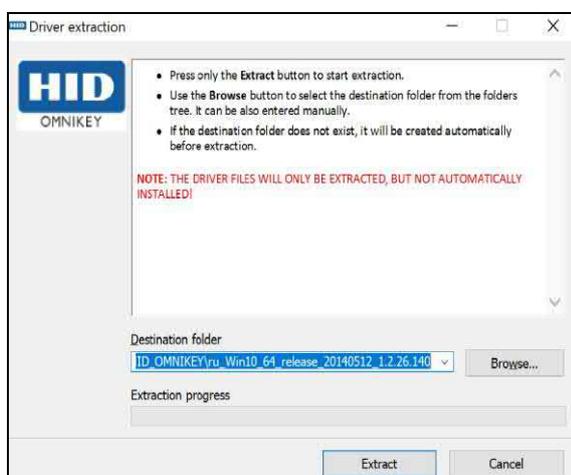


Abbildung 41: Treiberinstallation für Codierstation

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


SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

5 Xesar 3.0 Programme

Zur Verwaltung der Xesar-Anlage benötigen Sie die Xesar-Software sowie folgende Programme:

Xesar-Installation Manager

Mit dem Xesar-Installation Manager werden folgende Aufgaben durchgeführt:

- Starten und Stoppen des Servers
- Verwaltung der AdminCard
- Software Updates
- Verwalten von mehreren Anlagen
- Einlösen von KeyCredits und Keycredit Xesar-Lifetime Lizenzen.

Download der Xesar-Software (Xesar-Installation Manager) auf der EVVA Webseite (im Tab **Software und Identmedien**).



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

Xesar-Periphery Manager

Der Xesar-Periphery Manager ermöglicht den Betrieb der Codierstation am Client Rechner.

Der Download des Xesar-Periphery Managers ist in der Xesar-Software unter der Kachel **Support / Aktualisierung**.

Download-Anforderungsformular (siehe Abbildung):



[Download Xesar-Software](https://www.evva.com/at-de/xesar-software-download/?no_cache=1)

(https://www.evva.com/at-de/xesar-software-download/?no_cache=1)

Download Xesar-Software

Bitte füllen Sie dieses Formular aus und starten Sie dann mit dem Download der Xesar-Software.

Ihre Kontaktdaten

Anrede *	Titel
<input type="text" value="Herr"/>	<input type="text"/>
Vorname *	Nachname *
<input type="text"/>	<input type="text"/>
Anwender oder Fachhändler *	
<input type="radio"/> Anwender	
<input type="radio"/> Fachhändler	
Firma *	
<input type="text"/>	
Telefon	E-Mail *
<input type="text"/>	<input type="text"/>
Objektklasse	Subjektklasse
<input type="text" value="Bitte wählen"/>	<input type="text" value="Bitte wählen"/>
Anzahl der Türen	Anzahl der Türen mit elektronischen Zutritt
<input type="text" value="Bitte wählen"/>	<input type="text" value="Bitte wählen"/>

Abbildung 42: Download Xesar-Software

Sie erhalten eine E-Mail mit einem temporären Download-Link.

» Klicken Sie auf den Download-Link, um die Xesar-Software auszuwählen.

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service



Abbildung 43: Xesar-Software Download

» Laden Sie die ausgewählte Datei herunter.



Der Download des Xesar-Installation Managers kann bis zu 2 Minuten dauern.

5.1 Xesar-Installation Manager

Nach dem Download installieren Sie den Xesar-Installation Manager. Dazu gehen Sie wie folgt vor:

» **1. Schritt:**

Entpacken Sie die zip-Datei mit Rechtsklick auf die zip-Datei. Im Kontextmenü wählen Sie **Alle extrahieren** (ggf. **Hier entpacken**).

Es wird ein neuer entzippter Ordner erstellt, der den gleichen Namen, wie die zip-Datei hat.



Das Entpacken kann einige Minuten dauern.

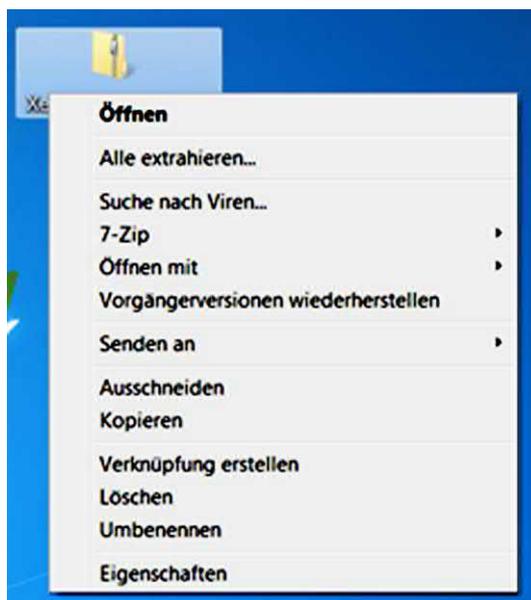


Abbildung 44: Xesar-Installation Manager zip-Datei

» 2. Schritt:

Öffnen Sie den Ordner (mit Doppelklick) und starten Sie die Anwendung **Installationmanager** (exe-Datei).

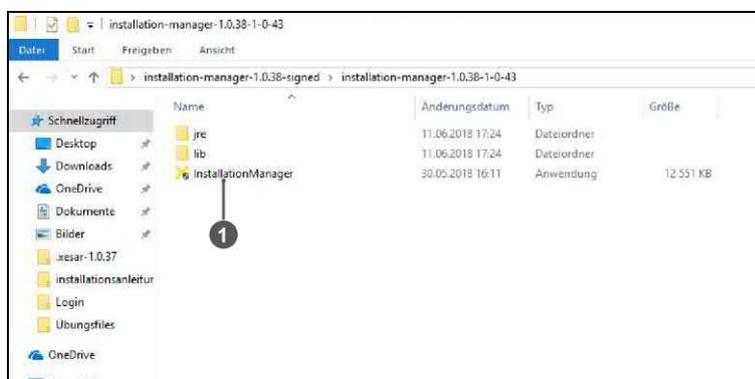


Abbildung 45: Xesar-Installation Manager Anwendung



Die Anwendungsdatei InstallationManager (.exe) darf **nicht** gelöscht oder an einen anderen Ort verschoben werden.



Der Xesar-Installation Manager darf nicht von einem Netzwerk gestartet werden, sondern muss auf einem lokalen Laufwerk liegen.



Um den Xesar-Installation Manager am Desktop zu starten, erstellen Sie eine Verknüpfung.

Falls die angezeigte Warnung betreffend Xesar-Installation Manager.exe erscheint, lassen Sie die Änderungen an Ihrem Gerät zu. Bestätigen Sie die Meldung mit **Ja**.



Abbildung 46: Xesar-Installation Manager – Warnmeldung

Der Xesar-Installation Manager wird geöffnet.

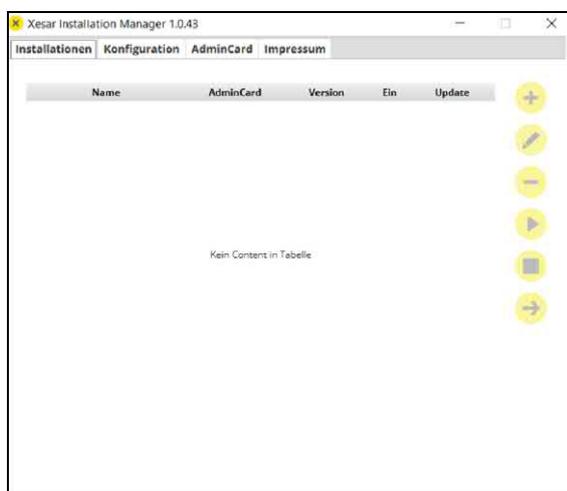


Abbildung 47: Xesar-Installation Manager

» 3. Schritt:

Leseinheit im Xesar-Installations Manager laden.

Klicken Sie auf den Reiter **AdminCard** ①.

Die Codierstation kann sowohl kontaktbehaftet (AdminCard) als auch kontaktlose CL-Smartcards (alle Xesar-Identmedien) lesen und verarbeiten. Für den Xesar-Installation Manager und das Lesen der AdminCard wird nur der kontaktbehaftete Leser benötigt.



Falls das Synchronisieren nicht funktioniert, wählen Sie den kontaktbehafteten Leser im Dropdown-Menü ❷ aus und klicken Sie auf Synchronisieren ❸.

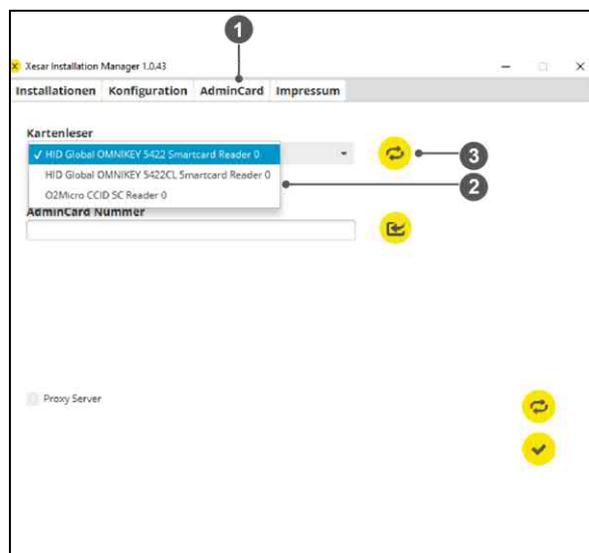


Abbildung 48: Leseinheit im Xesar Installation Manager laden

» 4. Schritt:

AdminCard laden.

Stecken Sie die AdminCard in den Slot der Codierstation und klicken Sie auf das Symbol **Laden** ❶. Speichern Sie ❷.

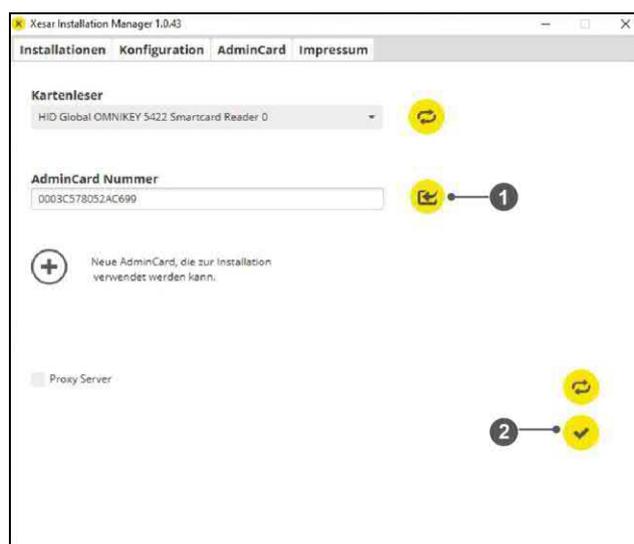


Abbildung 49: AdminCard laden



Der folgende Schritt gilt nur für Upgrades von Xesar 2.0 auf Xesar 3.0.

- » Stecken Sie die AdminCard Ihrer Xesar 2.2-Anlage in die Codierstation. Wenn die Meldung erscheint, können Sie Ihre Xesar 2.2-Daten importieren.

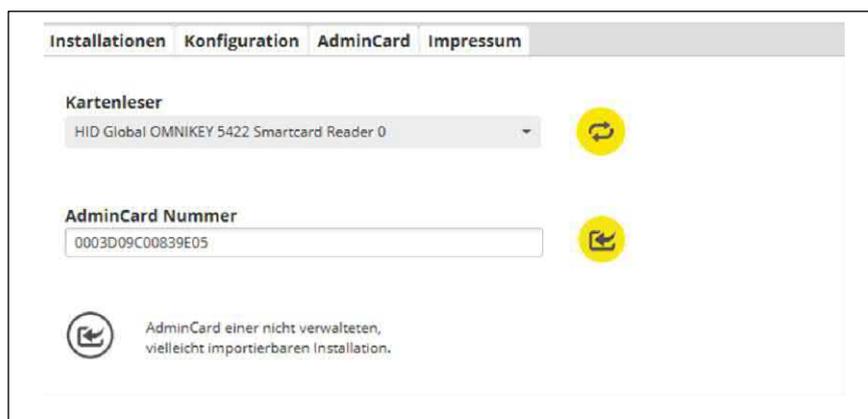


Abbildung 50: Xesar-Installation Manager - AdminCard importieren

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

» **5. Schritt:**

Neueste Xesar-Version laden.

Klicken Sie auf den Reiter **Konfiguration** ①,
bestätigen Sie **TLS Prüfen** ② und
klicken Sie auf **Synchronisieren** ③.

Es wird automatisch die neueste Version geladen und als Auswahl markiert. Prüfen
Sie das im Dropdown-Menü unter **Version** und klicken Sie auf **Speichern** ④.

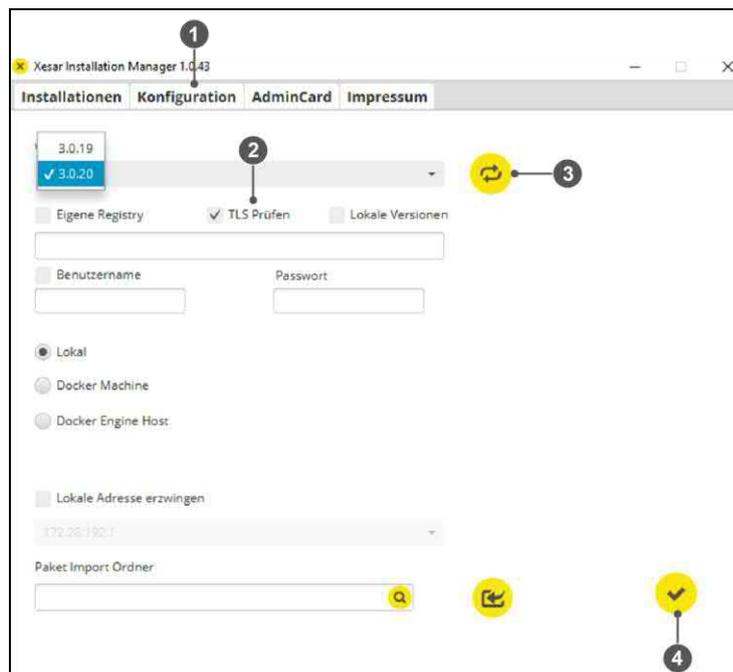


Abbildung 51: Laden

» **6. Schritt:**

Eine neue Anlage anlegen

Klicken Sie auf den Reiter **Installationen** ①,
klicken Sie auf das Symbol für **Hinzufügen** ②

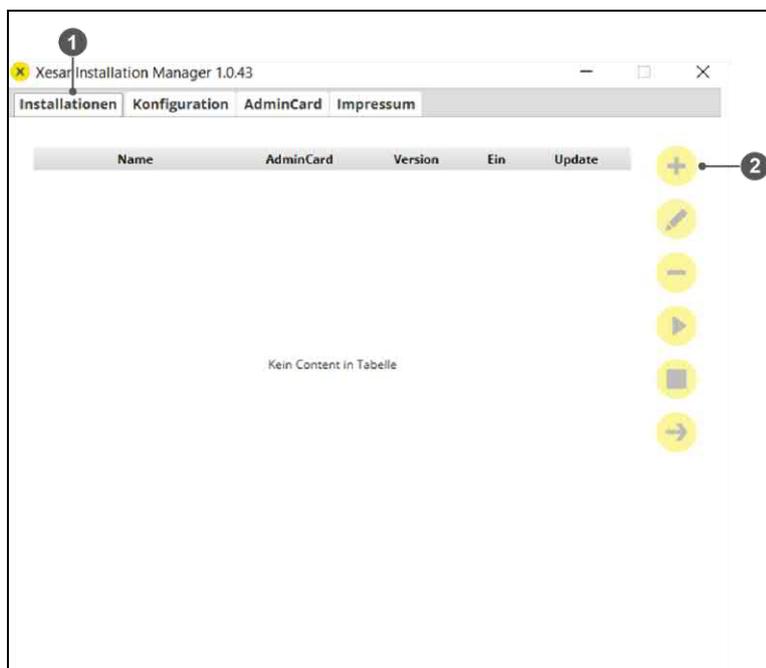


Abbildung 52: Eine neue Anlage anlegen

» **7. Schritt:**

Anlagen-Spezifikationen festlegen

Geben Sie den Anlagennamen ① ein (Sonderzeichen sind erlaubt, das \$-Zeichen ist nicht möglich) und fügen Sie eine zusätzliche Beschreibung hinzu.

Die eingetragenen Ports ② müssen in der Anlage frei sein, die Option **Local** ist als Defaultwert voreingestellt.

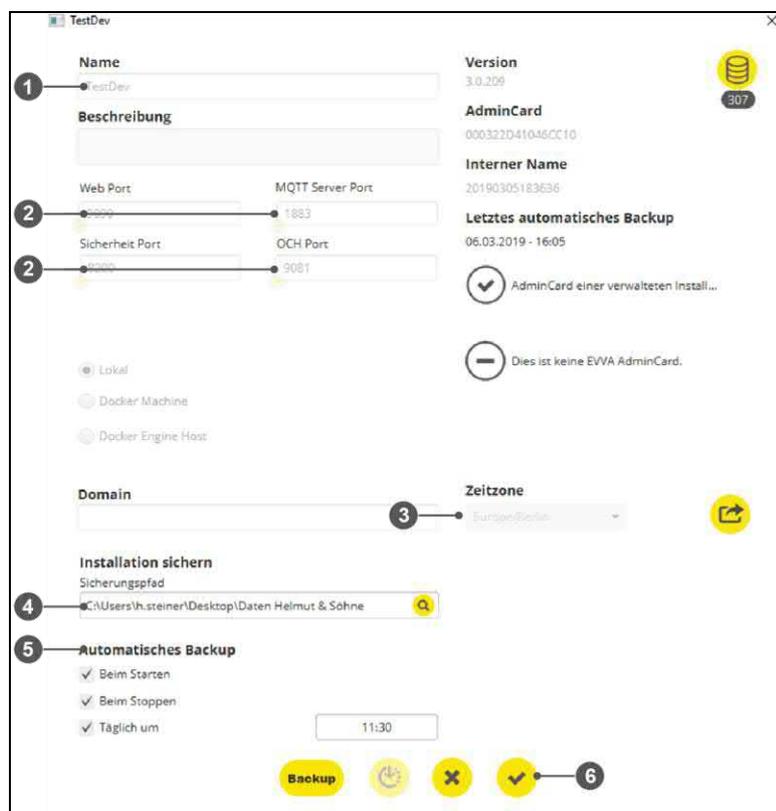
Wählen Sie Ihre Zeitzone ③ aus dem Pull-down Menü.



Die Zeitzone kann nachträglich nicht mehr geändert werden!

Geben Sie den Pfadnamen für Ihre Datensicherung ④ ein und legen Sie die Einstellungen für automatische Backups ⑤ fest.

Klicken Sie auf **Bestätigen** ⑥, um den Installationsprozess zu initialisieren.



» **8. Schritt:**

Notieren Sie sich den Web-Port.

Sie brauchen diese Daten später für die Konfiguration Ihres Xesar-Tablets.



Der folgende Schritt gilt nur für Upgrades von Xesar 2.0 auf Xesar 3.0.

» Datenimport Ihrer Xesar 2.2-Anlage:

Geben Sie den Namen der Datei ist aesssdb.h2 oder aesssdb.h2.db im Feld **Import** ① ein.

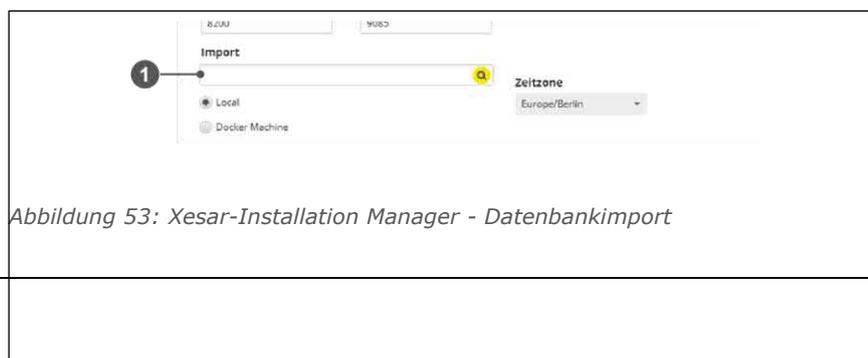


Abbildung 53: Xesar-Installation Manager - Datenbankimport

Ihre Xesar 3.0-Anlage wurde erfolgreich installiert.

» **9. Schritt:**

Installationsinformationen: Anlagenadministrator und Passwort



Nach erfolgreicher Installation der Anlage wird ein Übersichtsblatt mit Installationsinformationen generiert und automatisch geöffnet.

Beachten Sie die Passwörter für den Anlagenadministrator (admin) und den Systemadministrator (su).

Melden Sie sich mit dem Benutzernamen **admin** für den Anlagenadministrator und dem entsprechenden Passwort im Login an.

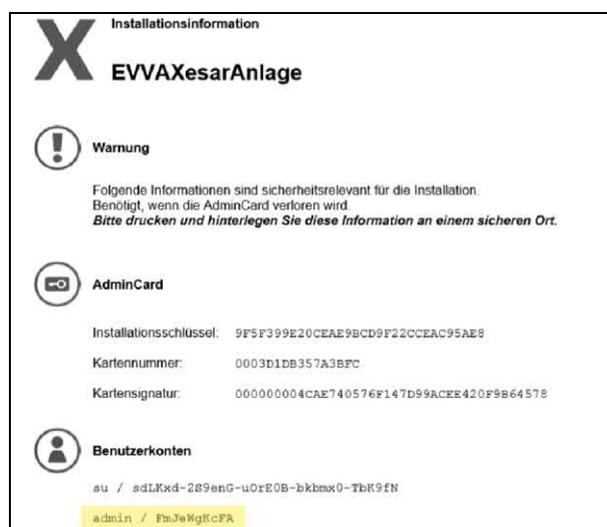


Abbildung 54: Installationsinformationen zur Anlage



Achtung!

Drucken Sie die Informationen aus und verwahren Sie den Ausdruck an einem sicheren Ort.

Bei Verlust oder Defekt der AdminCard sind die Informationen auf der Installationsinformation die einzige Möglichkeit, die Anlage weiter zu betreiben.

EVVA kann keine Wiederherstellung der Daten durchführen, wenn die Installationsinformationen der Anlage fehlen!



Falls das Übersichtsblatt mit den Installationsinformationen zur Anlage nicht automatisch geöffnet wird, gehen Sie wie folgt vor:

Klicken Sie auf den Reiter **Konfiguration**,
klicken Sie auf das Symbol **Exportieren** ①.

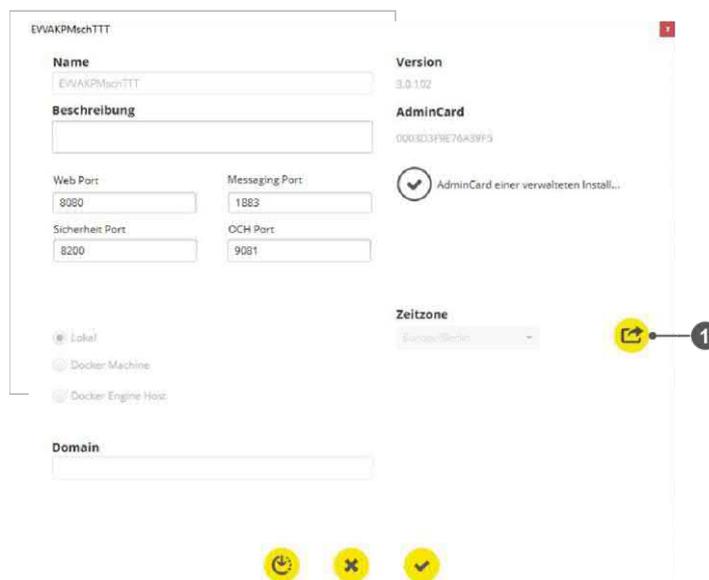


Abbildung 55: Anlageninformationen exportieren

Die Informationen werden auch als pdf-Datei unter C:\Users\Xesar\.xesar-1.0.43\Anlagenname ① gespeichert.

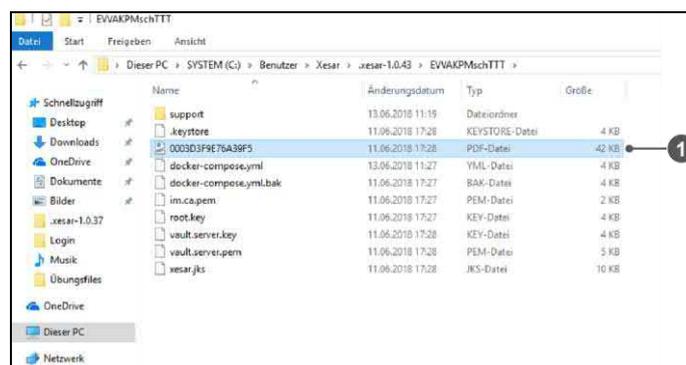


Abbildung 56: Anlagerinformationen

» 10. Schritt: Anlage starten

Die Installation ist erfolgreich abgeschlossen, wenn die Anlage als Listeneintrag erscheint. Das Symbol bedeutet, dass die Software noch nicht gestartet wurde.

Markieren Sie die Listenzeile Ihrer Anlage und klicken Sie auf das Symbol **Starten** ①.

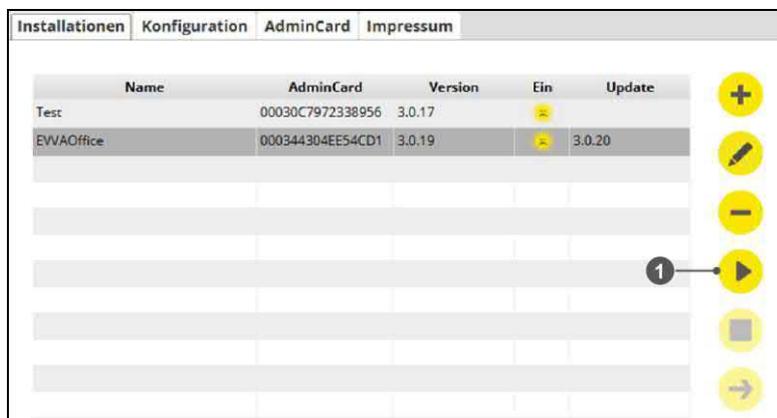


Abbildung 57: Software noch nicht gestartet

Der Startvorgang wird in der Fortschrittsanzeige ② dargestellt.



Abbildung 58: Anlage wird geladen

Das Symbol ☺ bedeutet, dass die Anlage läuft.

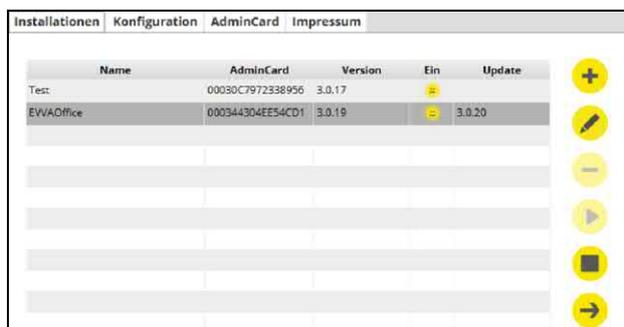


Abbildung 59: Anlage läuft

» **11. Schritt:**
KeyCredits aufladen

Klicken Sie auf das Symbol **Bearbeiten** ①

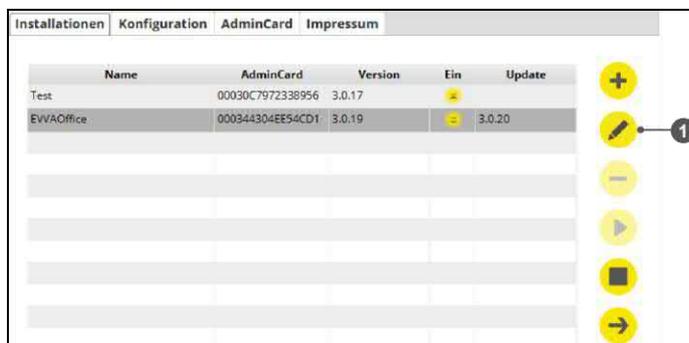


Abbildung 60: KeyCredits aufladen und aktivieren

Klicken Sie auf das Symbol **KeyCredits-Container** ②

Geben Sie Ihren **KeyCredits-Code** ③ ein. (Der KeyCredits-Code befindet sich auf der Rückseite der Rubbelkarte.)

Klicken Sie auf **Bestätigen** ④.



Abbildung 61: KeyCredits-Code eingeben

Wenn das Aufladen erfolgreich abgeschlossen wurde, erhalten Sie folgende Meldungen vom EVVA-Lizenzserver:

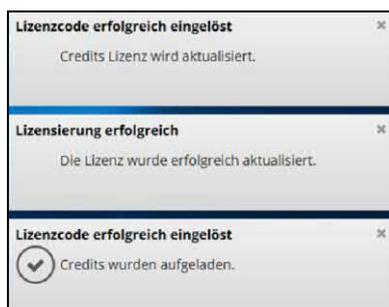


Abbildung 62: Meldungen vom EVVA-Lizenzserver



Für das Einlösen von KeyCredits ist eine bestehende Internetverbindung zum EVVA-Lizenzservice nötig!

Wenn eine KeyCredit Xesar Lifetime Lizenz eingelöst wird, erscheint folgende Anzeige:



Abbildung 63: KeyCredit Xesar-Lifetime

» 12. Schritt:

Xesar-Software-Dashboard

Das Symbol ☺ bedeutet, dass die Anlage läuft.

Klicken Sie auf das Symbol **Pfeil 1**, um zum Xesar-Dashboard zu gelangen.

Schließen Sie den Xesar-Installation Manager **2**. Die Anwendung läuft im Hintergrund weiter.



Mit dem Symbol **Stop 3** wird der Betrieb der Anlage (Server) beendet.

Zum Starten und Stoppen des Servers muss die AdminCard in der Codierstation stecken!

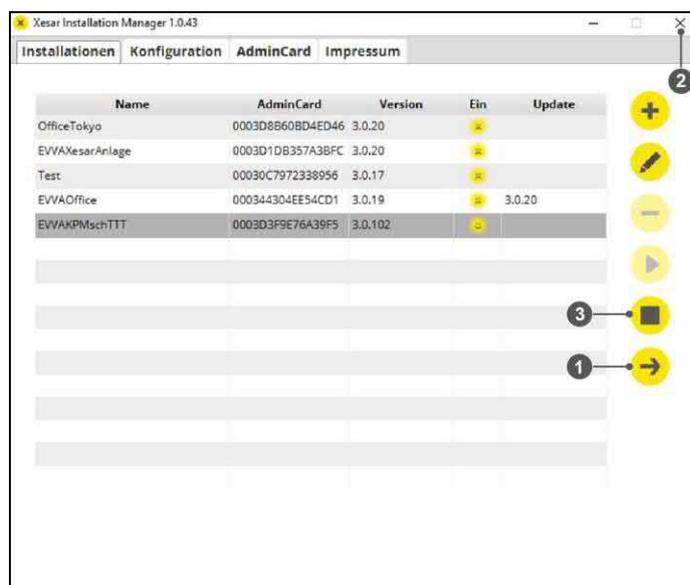


Abbildung 64: Xesar-Installation Manager – Funktionen

» **13. Schritt:**

Website laden



Warnhinweise von Ihrem Browser:

Sobald Xesar über den Pfeil aus dem Xesar-Installation Manager gestartet wird, werden Warnhinweise im verwendeten Browser eingeblendet!

Die Darstellung der Warnhinweise ist abhängig vom verwendeten Browser.

Klicken Sie auf Details ①



Abbildung 65: Warnhinweise im Browser

» **14. Schritt:**

Klicken Sie auf Webseite trotzdem laden

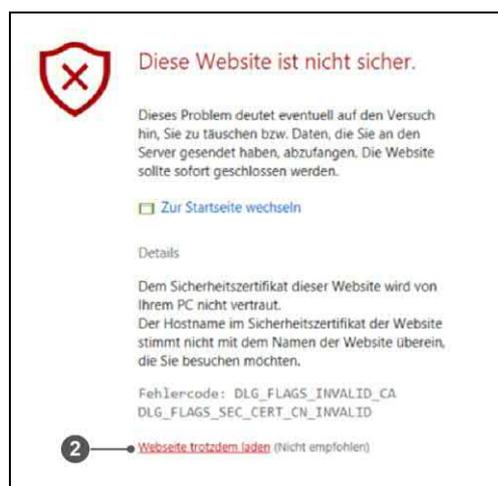


Abbildung 66: Warnhinweis im Browser

» **15. Schritt:**

Xesar-Software Login

Melden Sie sich mit dem Admin-Benutzernamen und Passwort im Login an.

Klicken Sie auf das Symbol **Pfeil 1**.

Beispiel:

Benutzername: admin

Passwort: FmJeWgKcFA



Abbildung 67: Login-Fenster

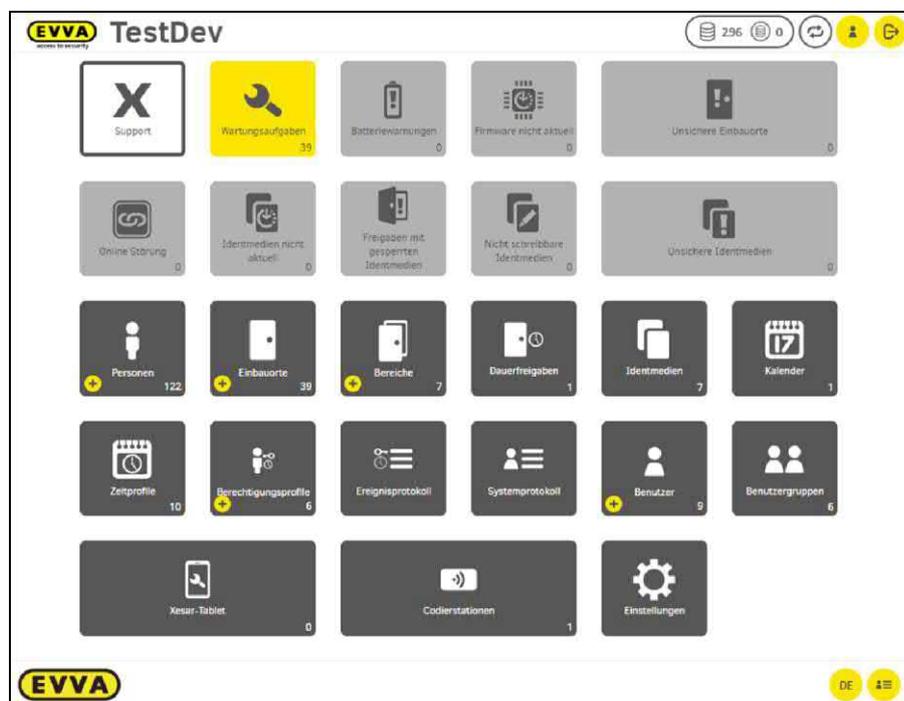


Abbildung 68: Xesar-Dashboard

5.2 AdminCard – Tausch

Die AdminCard kann bei Defekt oder Verlust wie folgt ausgetauscht werden:

- » Stecken sie eine **neue** AdminCard in die Codierstation.
- » Wählen Sie im Xesar-Installation Manager die gewünschte Anlage **1** aus und klicken Sie auf das Symbol **Schlüssel** **2**.

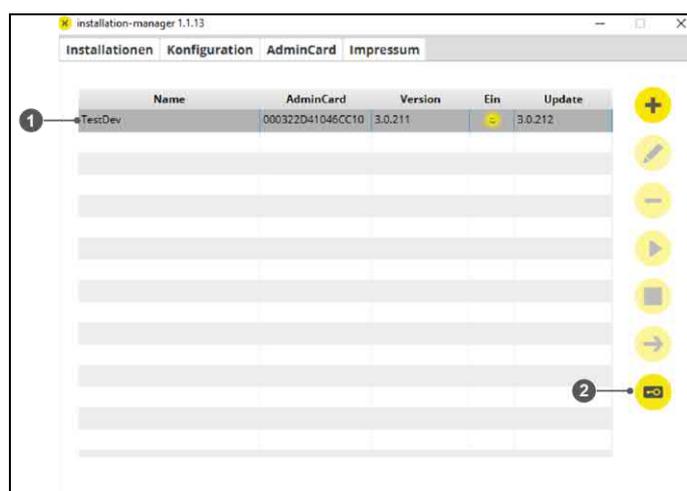
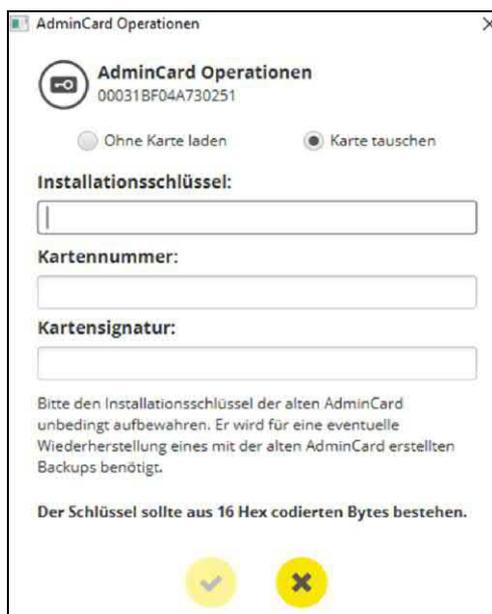


Abbildung 69: AdminCard tauschen

- » Wählen Sie im Fenster AdminCard Operationen die Funktion **Karte tauschen** und geben Sie den Installationsschlüssel, die Kartenummer und die Kartensignatur ein. (Die Daten stehen am Übersichtsblatt mit Installationsinformationen.)



AdminCard Operationen

AdminCard Operationen
00031BF04A730251

Ohne Karte laden Karte tauschen

Installationsschlüssel:

Kartenummer:

Kartensignatur:

Bitte den Installationsschlüssel der alten AdminCard unbedingt aufbewahren. Er wird für eine eventuelle Wiederherstellung eines mit der alten AdminCard erstellten Backups benötigt.

Der Schlüssel sollte aus 16 Hex codierten Bytes bestehen.

Abbildung 70: AdminCard tauschen

Nach der Bestätigung wird ein neues Übersichtsblatt mit Installationsinformationen generiert.

Drucken Sie dieses Übersichtsblatt mit Installationsinformationen aus und verwahren Sie es sicher.



Achtung!

Drucken Sie die Informationen aus und verwahren Sie den Ausdruck an einem sicheren Ort.

Bei Verlust oder Defekt der AdminCard sind die Informationen auf der Installationsinformation die einzige Möglichkeit, die Anlage weiter zu betreiben.

EVVA kann keine Wiederherstellung der Daten durchführen, wenn die Installationsinformationen der Anlage fehlen!



Nach dem Tausch Ihrer AdminCard führen Sie unbedingt ein **manuelles Backup** im Xesar-Installation Manager durch. Damit vermeiden Sie, dass ein Restore nicht mehr zur neuen AdminCard passt.

5.3 Xesar-Software Update

Wenn eine neue Xesar-Softwareversion verfügbar ist, wird im Xesar-Installation Manager die neue Softwareversion in der Zeile der Anlage  in der Spalte **Update** angezeigt.



Ab Version 3.0.212 können Updates auch mit noch offenen Wartungsaufgaben durchgeführt werden.



Vor einem Software-Update müssen alle **Tablets** der Anlage **abgemeldet** werden.

- » Bestätigen Sie, dass alle Tablets abgemeldet sind.



Abbildung 71: Xesar-Tablet abmelden

- » Wählen Sie die Anlage aus, für die Sie das Update durchführen möchten.
- » Klicken Sie auf das Symbol **Bearbeiten** ②. Die Seite Einstellungen wird geöffnet.

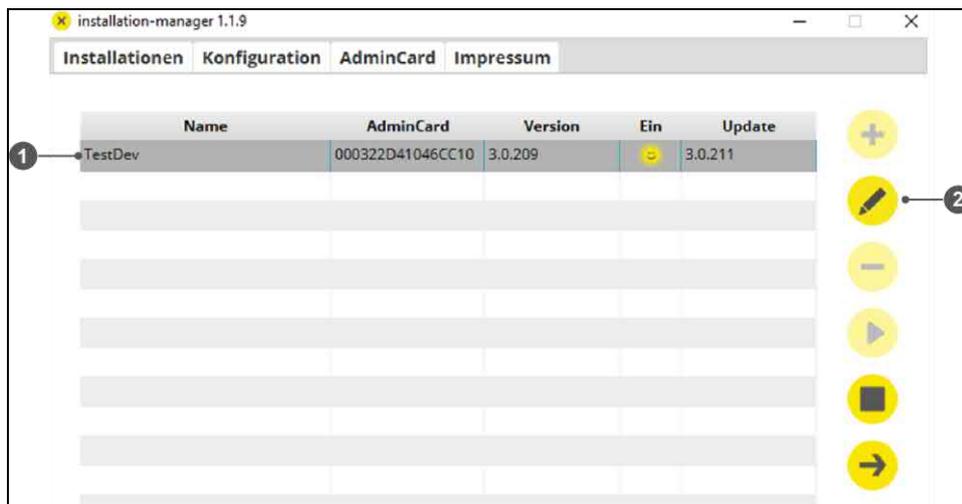


Abbildung 72: Xesar-Software Update

» Klicken Sie auf das Symbol **Update-Download** 3.

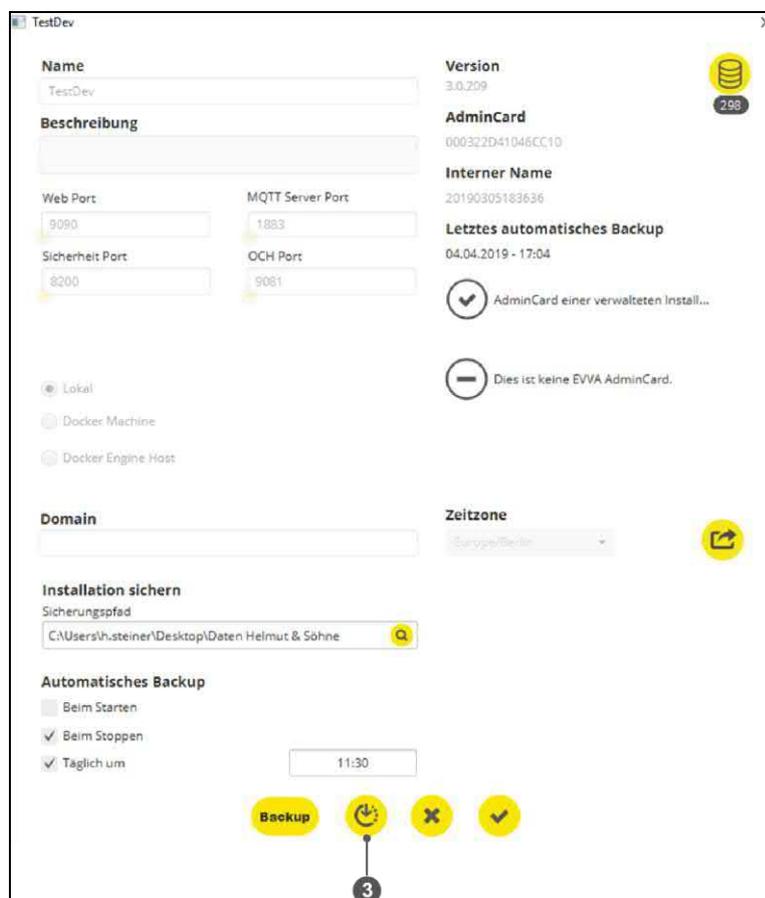


Abbildung 73: Xesar-Software Update durchführen



Vor einem Update wird zur Datensicherung ein automatisches Backup durchgeführt. Falls das Update nicht erfolgreich durchgeführt werden konnte, kann mit diesem Backup File eine Neuinstallation (Restore) der Anlage durchgeführt werden. (Siehe dazu Kapitel 3.12.4 Restore)

Es werden alle Änderungen der Versionen im Software Update angezeigt.

» Klicken Sie auf Bestätigen, um das Update zu starten.

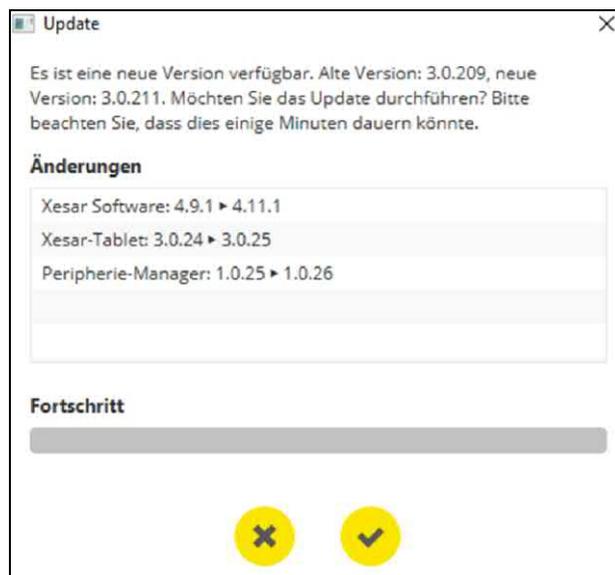


Abbildung 74: Xesar-Software Update

Es wird die automatische Anlagendatensicherung und anschließend das Update durchgeführt. Der Fortschritt wird angezeigt.



Abbildung 75: Installation sichern

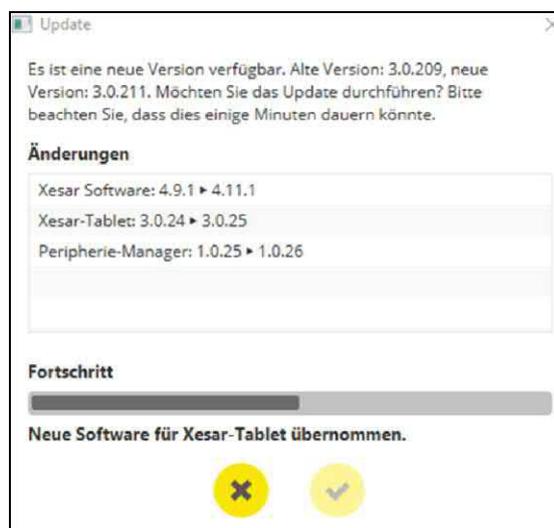


Abbildung 76: Xesar-Software Update

Wenn das Xesar-Software Update abgeschlossen ist, erhalten Sie eine entsprechende Meldung.



Abbildung 77: Meldung Update abgeschlossen

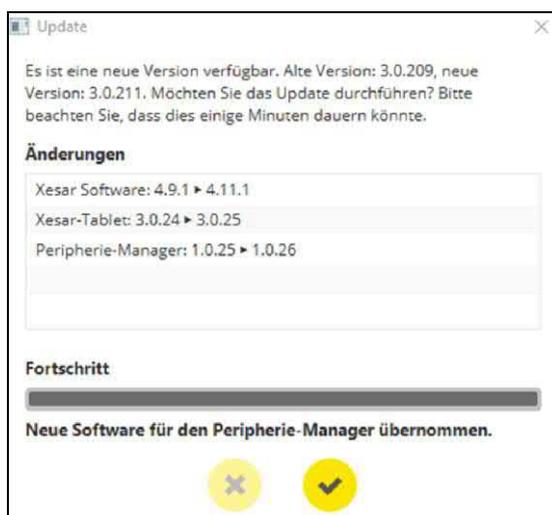


Abbildung 78: Meldung Update abgeschlossen

» Bestätigen Sie die Meldung, öffnet sich der Xesar-Installation Manager.

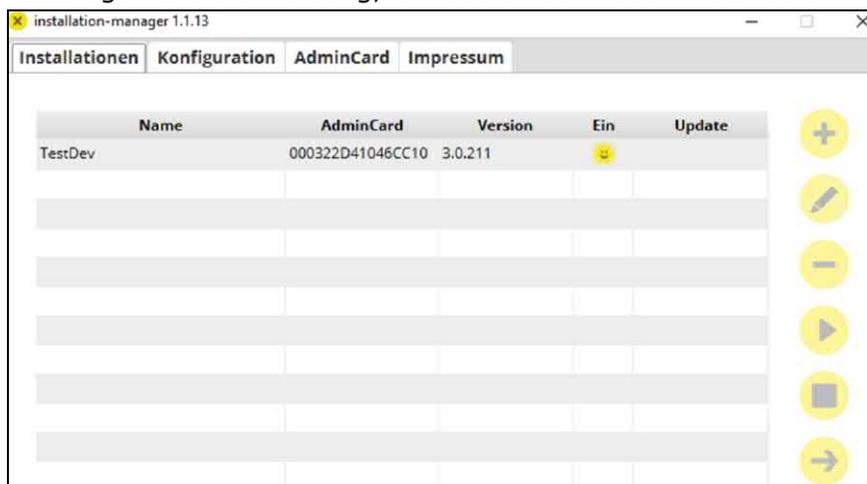


Abbildung 79: Installierte Version nach Update

5.3.1 Xesar-Installation Manager Update

Wenn eine neue Version des Xesar-Installation Managers verfügbar ist, wird beim Start des Xesar-Installation Managers folgende Meldung eingeblendet:



Abbildung 80: Xesar-Installation Manager Update

- » Geben Sie das Zielverzeichnis zur Installation des neuen Xesar-Installation Managers an.
- » Entzippen Sie die heruntergeladene Datei
- » Starten Sie den neuen Xesar-Installation Manager.

Verwenden Sie zukünftig nur mehr die neueste Version des Xesar-Installation Managers.


SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

5.4 Xesar-Periphery Manager

Der Xesar-Periphery Manager ermöglicht den Betrieb der Codierstation am Client Rechner. Mit der Codierstation werden die Identmedien der Anlagen erstellt, beschrieben, gelesen und aktualisiert.

» **1. Schritt:**

Support öffnen

Der Xesar-Periphery Manager befindet auf dem Xesar-Dashboard unter der Kachel Xesar-Support.

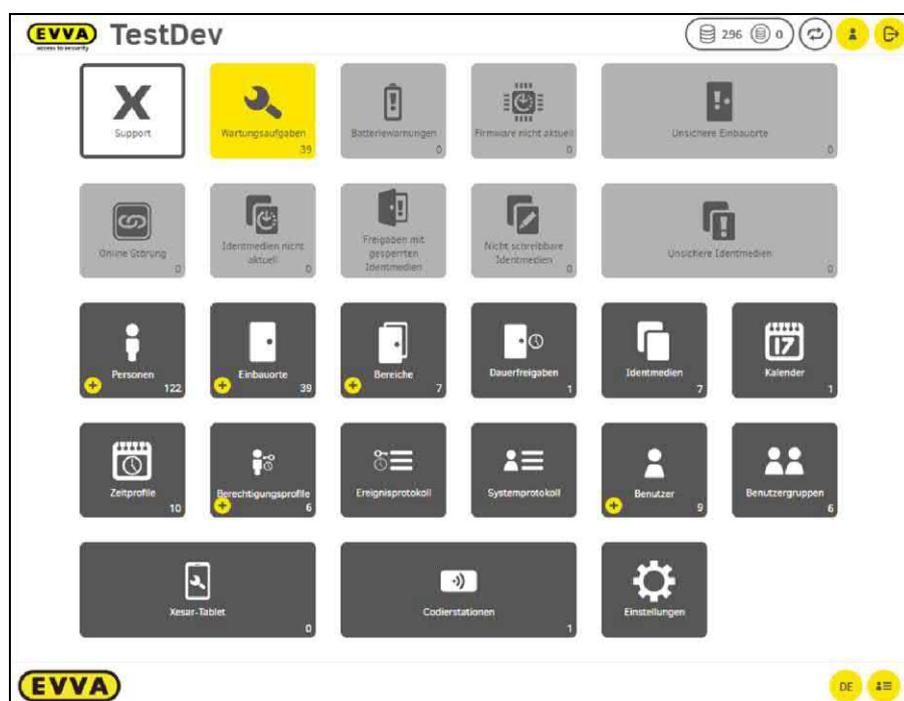


Abbildung 81: Xesar-Dashboard - Support wählen



Abbildung 82: Kachel Support

» **2. Schritt:**
Xesar-Peripherie Manager herunterladen

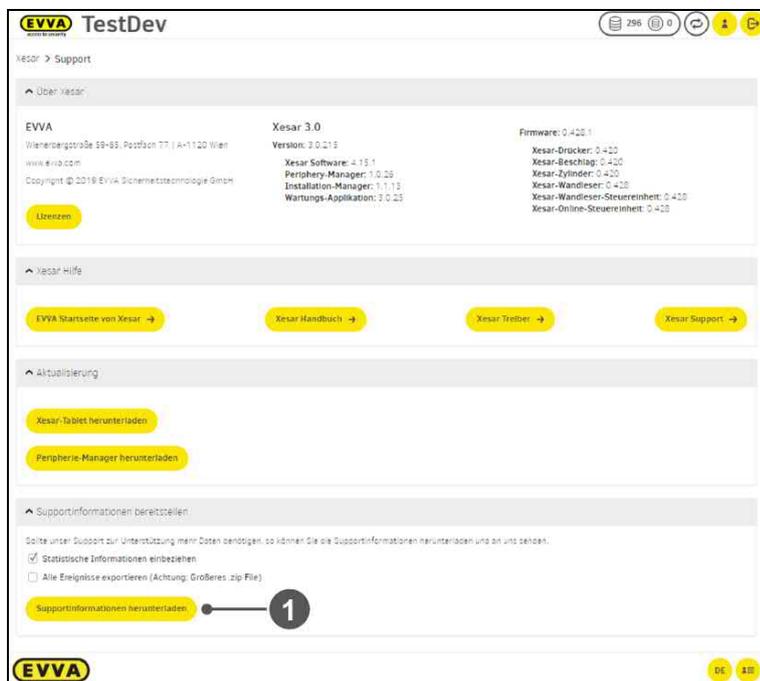


Abbildung 83: Xesar-Periphery Manager auswählen

» **3. Schritt:**
zip-Datei entpacken



Abbildung 84: Xesar-Periphery Manager – zip-Datei extrahieren

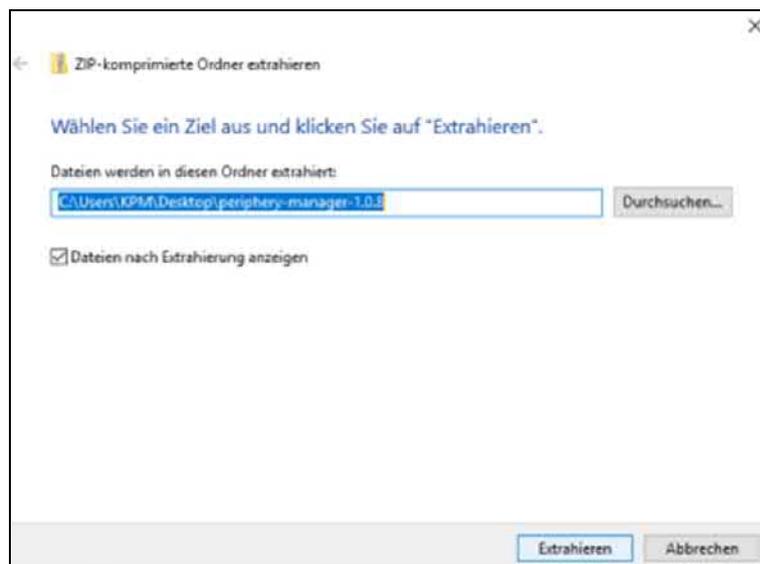


Abbildung 85: Xesar-Periphery Manager zip-Datei extrahieren

» 4. Schritt:

Anwendung ausführen

Ordner **periphery-manager x.x.x** öffnen (x.x.x. steht für die angezeigte Nummer – in unserem Beispiel 1.0.16).

Doppelklick auf die Anwendungsdatei **xesarPeriphery**.



Abbildung 86: Xesar-Periphery Anwendung

- » Falls die Windows-Warnmeldungen **Der Computer wurde durch Windows geschützt** angezeigt wird, klicken Sie auf **Weitere Informationen** ①.



Abbildung 87: Xesar-Periphery Anwendung - Warnmeldung

- » Klicken Sie auf **Trotzdem ausführen** ②.



Abbildung 88: Xesar-Periphery Manager Warnmeldung

Falls noch weitere Warnmeldungen betreffend die Installation des Xesar-Periphery Managers eingeblendet werden, akzeptieren Sie diese.

Das Programm wird installiert, der Xesar-Peripherie Manager wird geöffnet und ist nun einsatzbereit.

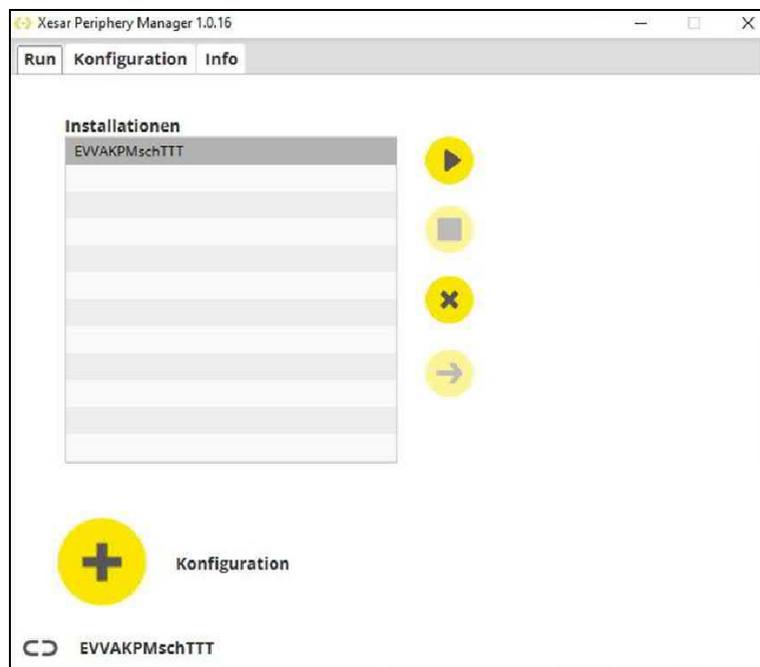


Abbildung 89: Xesar-Periphery Manager

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden
Dresdner Straße 177 · 01705 Freital
Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

5.5 Codierstation mit der Xesar-Software verknüpfen

Verknüpfen Sie die Codierstation mit der Xesar-Software. Dazu gehen Sie wie folgt vor:

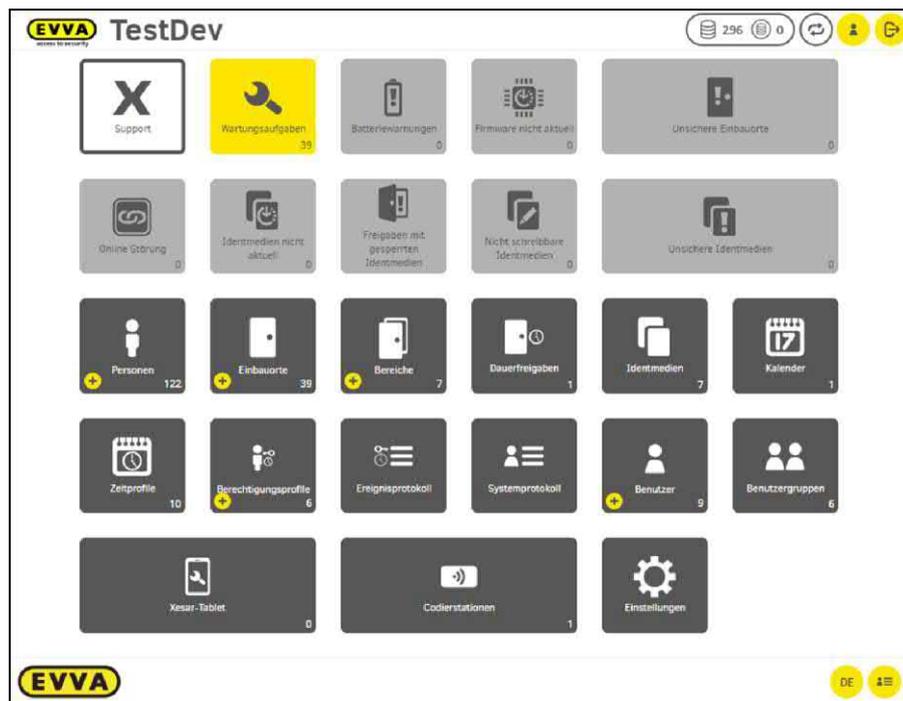


Abbildung 90: Codierstation am Xesar-Dashboard

» 1. Schritt:

Klicken Sie auf die Kachel Codierstationen



Abbildung 91: Kachel Codierstationen

» **2. Schritt:**

Codierstation hinzufügen

Klicken Sie auf das Symbol **+** ①, um eine neue Codierstation hinzuzufügen.



Abbildung 92: Codierstation Namen hinzufügen

» **3. Schritt:**

Codierstation benennen

Geben Sie Namen ① und eventuell eine Beschreibung ein und klicken Sie auf das Symbol **Bestätigen** ②.



Abbildung 93: Codierstation Status

Die Codierstation ist nun in der Übersichtsliste eingetragen, sie ist jedoch noch nicht mit dem Client-Rechner verbunden ③.



Abbildung 94: Codierstation Konfigurationsdatei Download

» **4. Schritt:**

Codierstation aktivieren und Konfigurationsdatei herunterladen

Klicken Sie auf den Listeneintrag der Codierstation

Wählen Sie die Option **Codierstation in diesem Browser verwenden** ①

Klicken sie auf das Symbol **Download** ② und laden Sie die Konfigurationsdatei der Codierstation herunter.

Klicken Sie zum Speichern Ihrer Eingaben auf das Symbol **Bestätigen** ③.

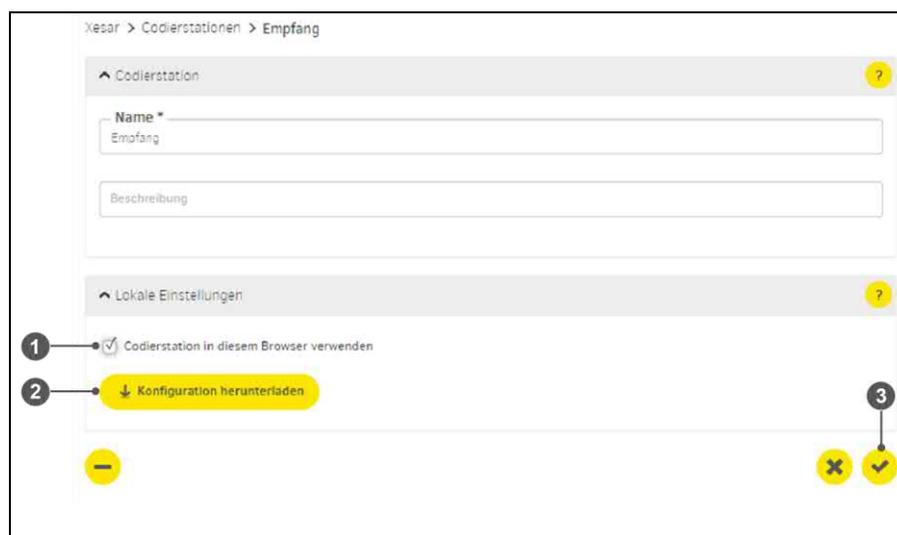


Abbildung 95: Xesar-Periphery Manager Konfigurationsdatei hinzufügen

» **5. Schritt:**

Konfigurationsdatei importieren

Klicken Sie im Xesar-Periphery Manager auf das Symbol **+** ①, um die Konfigurationsdatei zu importieren

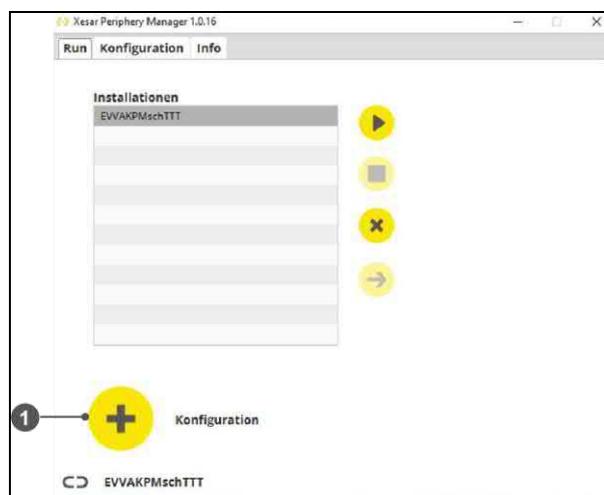


Abbildung 96: Xesar-Periphery Manager Konfigurationsdatei auswählen

.properties ② ist die Dateierdung der Konfigurationsdatei.

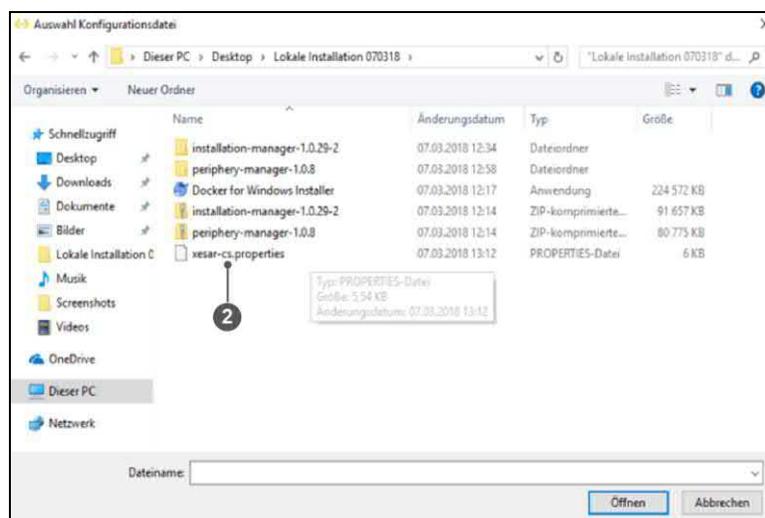


Abbildung 97: Xesar-Anlage im Xesar-Periphery Manager

Ihre Installation (der Name Ihrer Anlage) wird nun als Listeneintrag im Periphery Manager angezeigt.

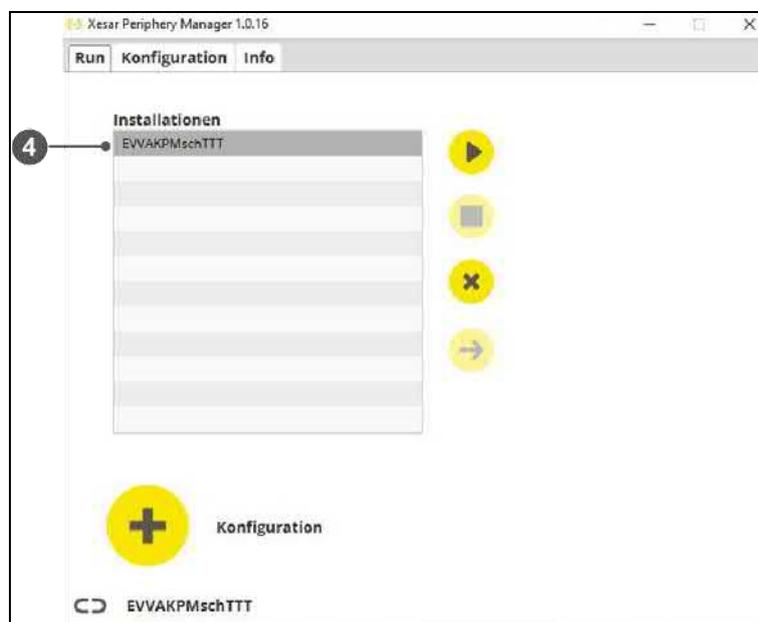


Abbildung 98: Xesar-Periphery Manager Auswahl der Codierstation

» **6. Schritt:**

Leseinheit wählen

Wählen Sie die Leseinheit mit der Bezeichnung **OMNIKEY mit CL** **1** aus.
Klicken Sie zum Speichern Ihrer Eingaben auf das Symbol **Bestätigen** **2**.

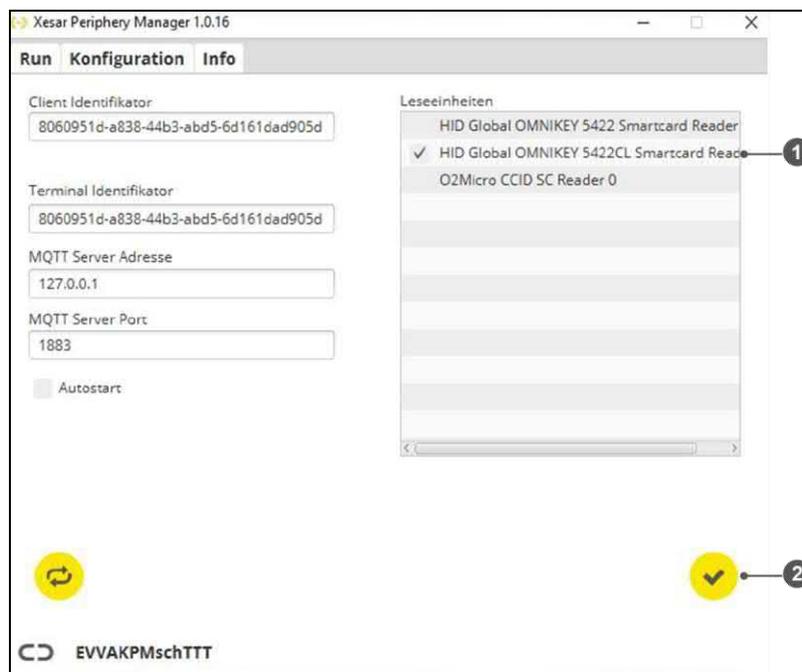


Abbildung 99: Xesar-Periphery Manager starten


SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden
Dresdner Straße 177 · 01705 Freital
Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

» **7. Schritt:**

Xesar-Periphery Manager starten

Wählen Sie den Tab „Run“ und klicken Sie auf das Symbol **Start**, um den Periphery Manager zu starten.

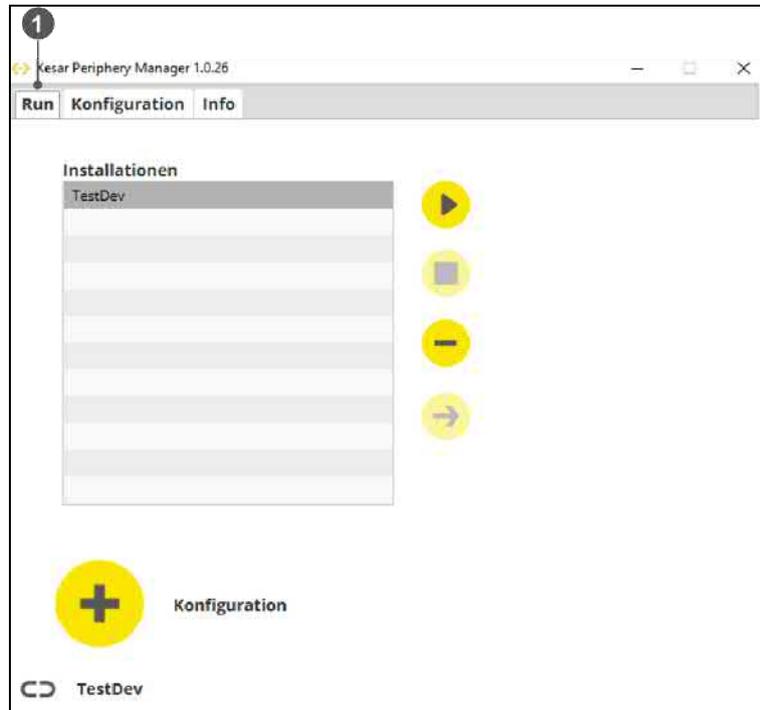


Abbildung 100: Xesar-Periphery Manager schließen

» **8. Schritt:**

Codierstation mit Xesar-Software verbinden.

Aktualisieren Sie die Xesar-Oberfläche im Browser (Funktionstaste F5 oder Strg+R). Die Codierstation ist nun mit dem Browser verbunden. (Status Verbunden: Ja)

Schließen Sie den Xesar-Periphery Manager (er läuft im Hintergrund weiter).

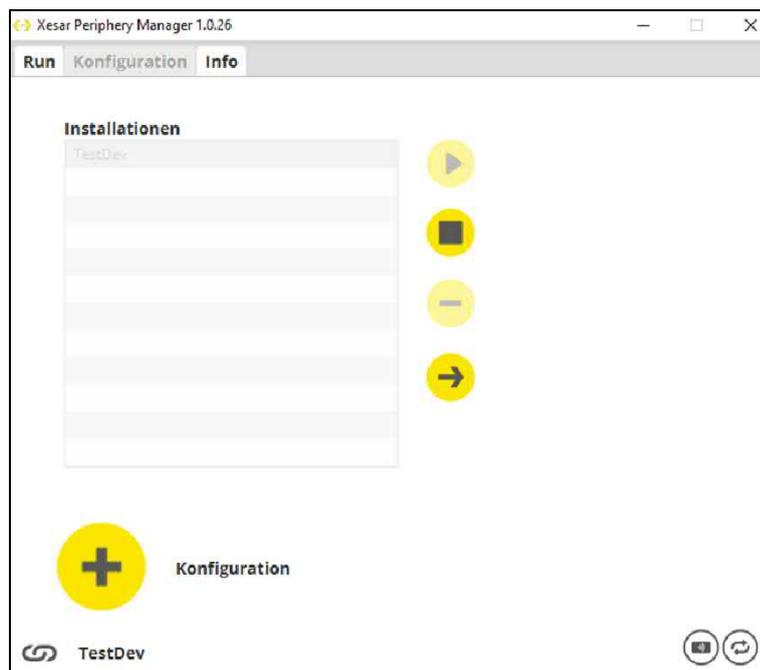


Abbildung 101: Codierstation mit Xesar-Software verbinden



Abbildung 102: Codierstation-Status Verbunden - Ja

Ihre Codierstation ist jetzt einsatzbereit.

5.6 Xesar-Tablet in Anlage einbinden

Das Xesar-Tablet wird mit der aktuellen Xesar-App ausgeliefert. Die Einrichtung des Tablets (erstmalige Synchronisation) mit der Anlage (PC) erfolgt über das gemeinsame WLAN (Wireless Local Area Network).

Im Betrieb wird das Xesar-Tablet mit der Xesar-Software ebenfalls über das gemeinsame WLAN synchronisiert.



Der folgende Schritt gilt nur für Upgrades von Xesar 2.0 auf Xesar 3.0.

Bereiten Sie zuerst Ihr Xesar-Tablet vor.

(Siehe 5.7 Manuelle Deinstallation und Installation der Xesar-App)

Die IP-Adresse des Rechners im WLAN wird als Server-Adresse im Xesar-Tablet mit der jeweiligen Port-Nummer (z. B. `https:// 172.31.16.85:8080`) angegeben.

» 1. Schritt:

Die richtige IP-Adresse finden

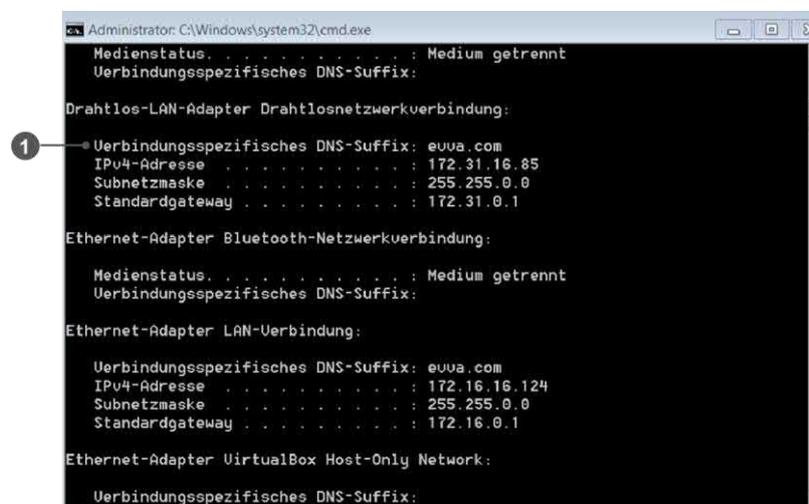
Geben Sie im Suchfenster von **cmd** ein, öffnet sich die Windows-Kommandozeile.

Geben Sie in der Kommandozeile den Befehl **ipconfig** ein und bestätigen Sie Ihre Eingabe mit **Enter**.

Scrollen Sie nach unten bis zu **Drahtlos-LAN-Adapter**

Drahtlosenetzwerkverbindung (oder – abhängig von Ihrer Hardware – z.B. Drahtlos-LAN-Adapter WiFi.)

Notieren Sie die IP-Adresse **von ihrem PC** in der Zeile **IPv4-Adresse** (evtl. auch IPv6) auf Ihrem Rechner angegeben ist. (In unserem Beispiel ist das 172.31.16.85.)



```
Administrator: C:\Windows\system32\cmd.exe
Medienstatus. . . . . : Medium getrennt
Verbindungsspezifisches DNS-Suffix:
Drahtlos-LAN-Adapter Drahtlosenetzwerkverbindung:
1 - Verbindungsspezifisches DNS-Suffix: evva.com
  IPv4-Adresse . . . . . : 172.31.16.85
  Subnetzmaske . . . . . : 255.255.0.0
  Standardgateway . . . . : 172.31.0.1

Ethernet-Adapter Bluetooth-Netzwerkverbindung:
Medienstatus. . . . . : Medium getrennt
Verbindungsspezifisches DNS-Suffix:
Ethernet-Adapter LAN-Verbindung:
Verbindungsspezifisches DNS-Suffix: evva.com
  IPv4-Adresse . . . . . : 172.16.16.124
  Subnetzmaske . . . . . : 255.255.0.0
  Standardgateway . . . . : 172.16.0.1

Ethernet-Adapter VirtualBox Host-Only Network:
Verbindungsspezifisches DNS-Suffix:
```

Abbildung 103: Windows Command-line CLI

» 2. Schritt:

Web Port-Nummer finden

Für das Xesar-Tablet benötigen Sie zusätzlich zur IP-Adresse die Port-Nummer. Diese ist ident mit der im Xesar-Installation Manager eingestellten Nummer (oder schreiben Sie die Nummer aus dem Browser ab, z.B.: `https:// 172.31.16.85:8080`.)

Alternativ finden Sie die Web Port-Nummer im Xesar-Installation Manager:

- » Klicken Sie auf das Symbol **Bearbeiten** im Xesar-Installation Manager. Notieren Sie die Web Port-Nummer ❶.

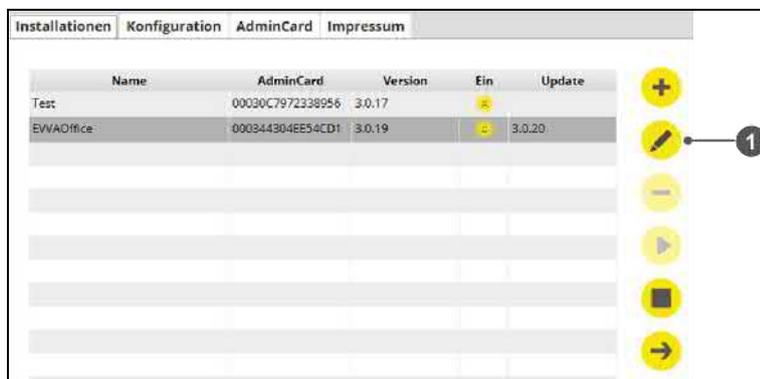


Abbildung 104: Xesar-Installation Manager Konfiguration

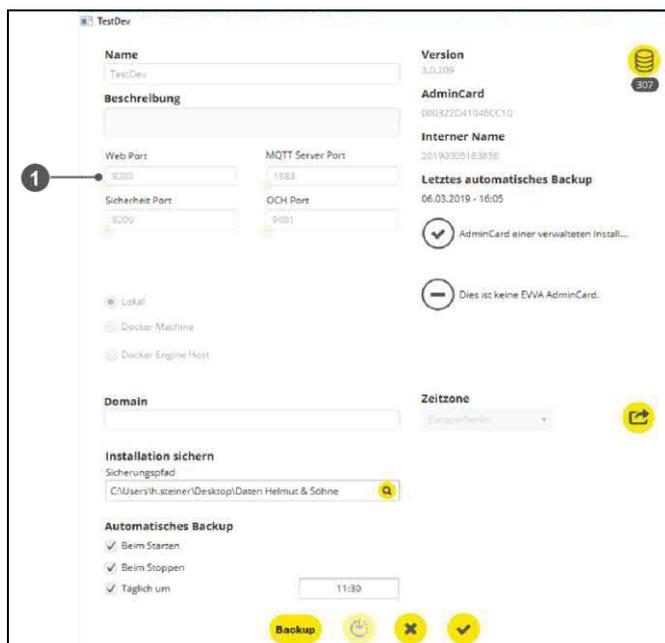


Abbildung 105: Xesar-Installation Manager Tablet Web Port

» 3. Schritt:

Öffnen Sie auf Ihrem Xesar-Tablet die Xesar-App.

Klicken Sie auf **Synchronisieren** und geben Sie Daten ein:

- in dem Feld **Xesar-Server** die vorher notierte IP Adresse **https://IPv4-Adresse-Ihres-Rechners:PortNr-Ihrer-Xesar-Anlage ①**, z. B. z.B.:
https://172.31.16.85:8080
- Name des Xesar-Tablets ②, z. B. **Wartungstechniker 1**
- Benutzernamen und Passwort ③, z. B. **Admin + Passwort**.



Der Benutzer muss der Berechtigungsgruppe Admin oder Wartungstechniker zugewiesen sein, um das Xesar-Tablet benutzen zu können.

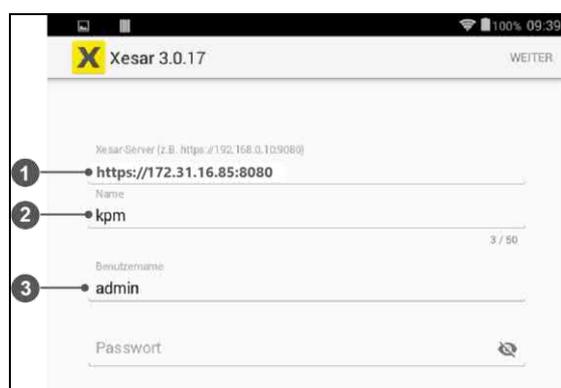


Abbildung 106: Tablet-App - Login

» 4. Schritt:

Zertifikat installieren

Klicken Sie auf Ja, installieren, um das Zertifikat zu installieren.



Abbildung 107: Xesar-Tablet – Zertifikat 1

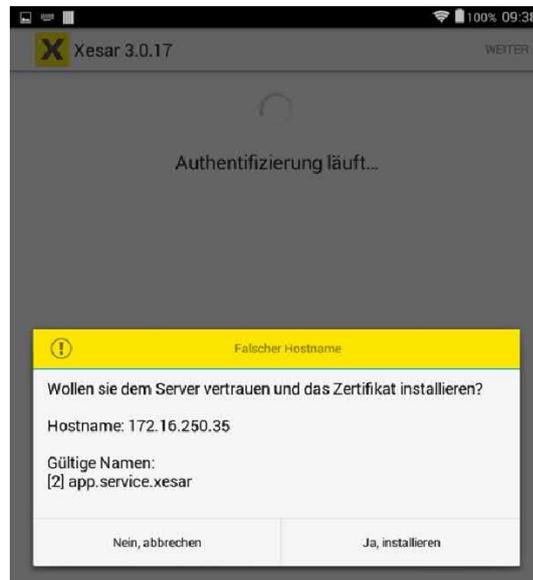


Abbildung 108: Xesar-Tablet – Zertifikat 2

Die Authentifizierung dauert nur wenige Sekunden.

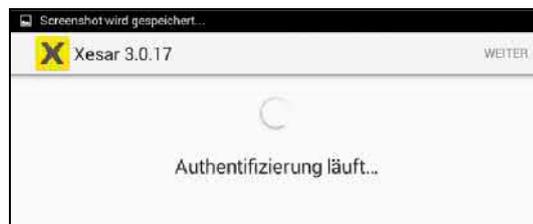


Abbildung 109: Authentifizierung Xesar-Tablet

Abhängig von der Menge der zu synchronisierenden Daten kann die Synchronisierung einige Minuten dauern.



Abbildung 110: Synchronisierung Xesar-Tablet



Abbildung 111: Tablet App Home

In der Xesar-Tablet Kachel am Xesar-Dashboard wird die Anzahl, der in der Anlage hinzugefügten Xesar-Tablets **1** angezeigt.

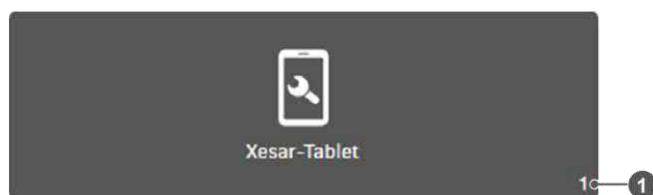


Abbildung 112: Kachel Xesar-Tablet

Damit haben Sie Ihr Xesar-Tablet in die Anlage integriert!
Sie können nun Ihre Anlage in der Xesar-Software konfigurieren.

Beachten Sie im Kapitel 7 die Informationen über Eingabe und Verwaltung der Systemeinstellungen, Zeitprofile, Berechtigungsprofile, Einbauorte mit Komponenten, Identmedien und Personen.

5.7 Manuelle Deinstallation und Installation der Xesar-App

(Upgrade von Xesar 2.2 auf Xesar 3.0)

Bei einem Upgrade von Xesar 2.2 auf Xesar 3.0 muss bei einem Xesar 2.2-Tablet die Xesar 2.2-App manuell deinstalliert und die Xesar 3.0-App manuell installiert werden.

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

» **1. Schritt:**

Klicken Sie auf **Einstellungen** ① im Hauptmenü

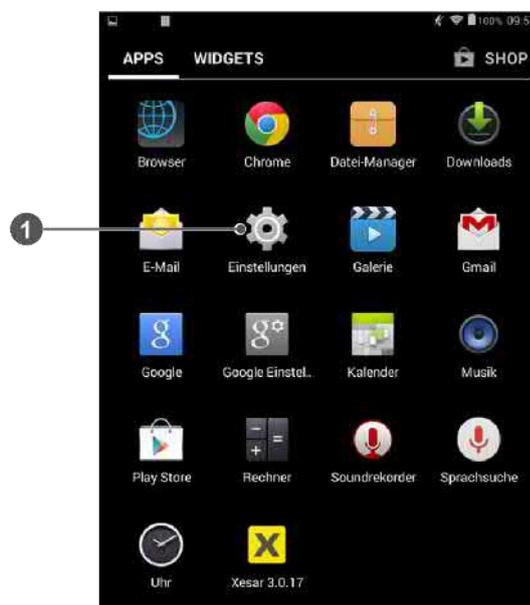


Abbildung 113: Xesar-Tablet Einstellungen

- » **2. Schritt:**
Klicken Sie auf **Apps** ①.

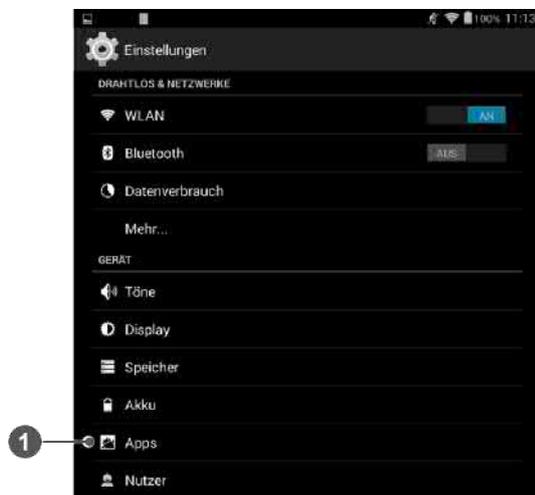


Abbildung 114: Xesar-Tablet Einstellungen App

- » **3. Schritt:**
Deinstallieren ① Sie die Xesar 2.2-App.



Abbildung 115: Xesar-Tablet Xesar-App deinstallieren

» **4. Schritt:**

Klicken Sie auf Ok.



Abbildung 116: Xesar-Tablet App deinstallieren OK

» **5. Schritt:**

Öffnen Sie den Dateimanager Ihres Xesar-Tablets ①.

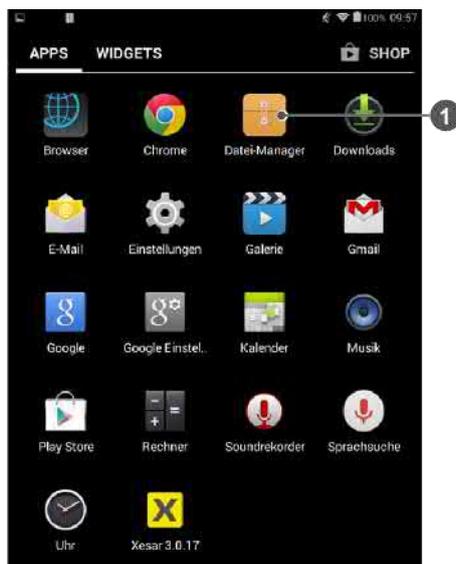


Abbildung 117: Xesar-Tablet Datenmanager

» **6. Schritt:**

Klicken Sie auf den Ordner **Download** und löschen Sie dort die .apk-Datei ①.

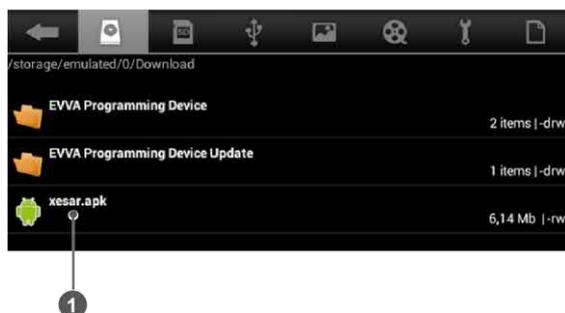


Abbildung 118: Xesar-Tablet APK löschen

» **7. Schritt:**

Klicken Sie am Xesar-Dashboard auf die Kachel **Support**.

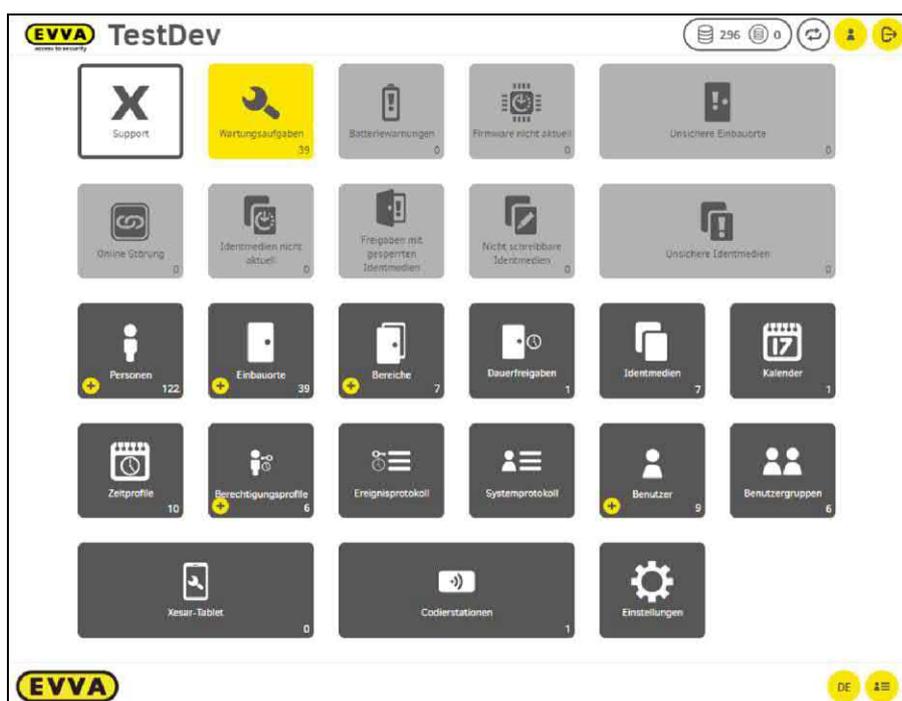


Abbildung 119: Desktop – Support auswählen



Abbildung 120: Kachel Support

» **8. Schritt:**

Xesar-Tablet herunterladen:

Laden Sie die aktuelle Xesar-App unter **Aktualisierung** herunter.

Klicken Sie auf **Xesar-Tablet herunterladen** ①.

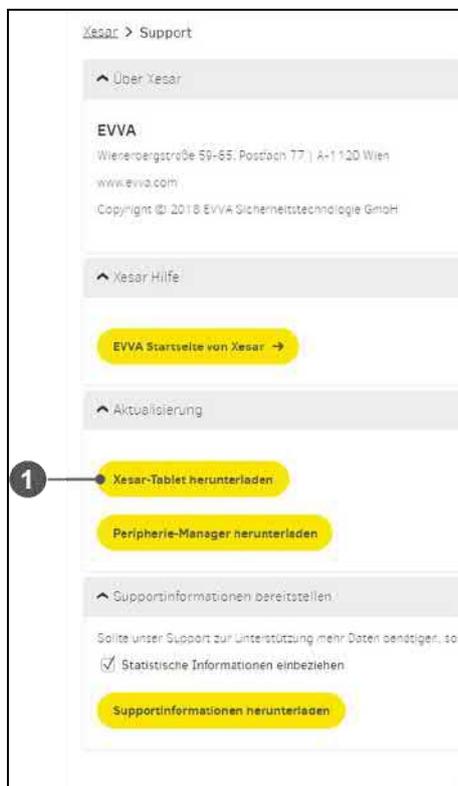


Abbildung 121: Xesar-Periphery Manager auswählen

» **9. Schritt:**

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



Abbildung 122: Xesar-Tablet APK-Datei

» **10. Schritt:**

Klicken Sie auf die .apk-Datei ①, um die Xesar-App auf Ihrem Xesar-Tablet zu installieren.

Klicken Sie auf **Installieren** ②.

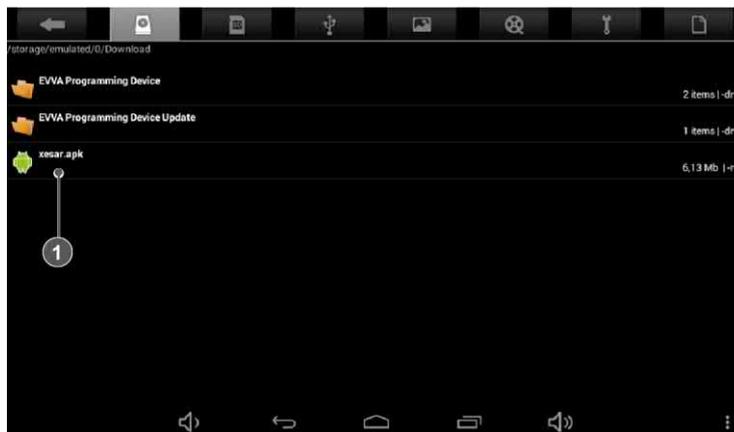


Abbildung 123: Xesar-Tablet - Xesar 3.0-App

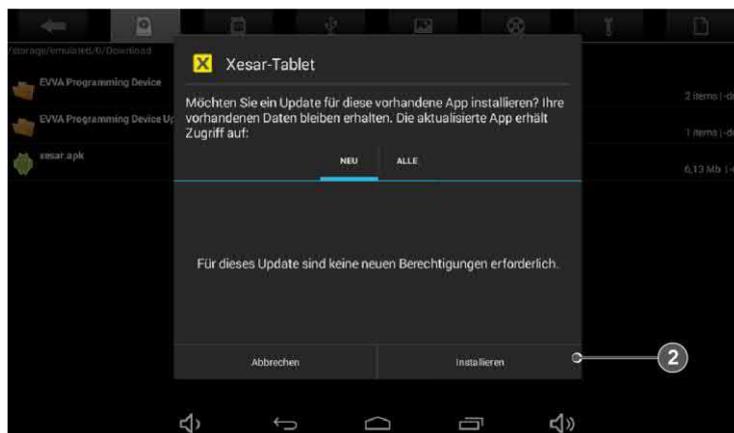


Abbildung 124: Xesar-Tablet - Xesar 3.0-App installieren

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

» **11. Schritt:**

Synchronisieren Sie anschließend das Xesar-Tablet mit der Xesar-Software.



Abbildung 125: Xesar-Tablet synchronisieren

» **12. Schritt:**

Schließen Sie die Einbindung des Xesar-Tablets in Xesar 3.0 ab.

Führen Sie die Schritte lt. Kapitel 5.6, Xesar-Tablet in Anlage einbinden, aus.


SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

6 Sicherung der Xesar-Anlagendaten im Xesar-Installation Manager



Zur erfolgreichen Datensicherung muss ein erreichbarer Backup-Speicherort angegeben sein.

6.1 Manuelles Backup

Ein manuelles Backup ist jederzeit möglich. Die AdminCard muss in der Codierstation stecken und ausgewählt sein. Wenn die Anlage gestoppt ist und im Xesar-Installation Manager der Backup- Button gedrückt wird, wird die Anlage gestartet, das Backup durchgeführt und die Anlage nach erfolgreichem Backup wieder gestoppt.

Gehen Sie wie folgt vor:

» 1. Schritt:

Wählen Sie im Xesar-Installation Manager die zu sichernde Anlage aus ❶ und klicken Sie auf das Symbol **Bearbeiten** ❷, um die Einstellungsseite zu öffnen.

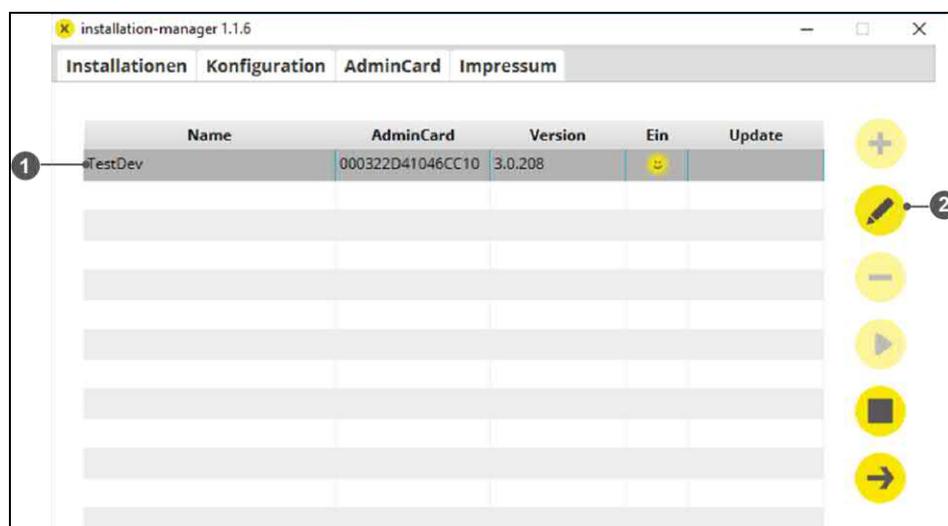


Abbildung 126: Manuelles Backup

» 2. Schritt:

Geben Sie den Sicherungspfad ❶ für Ihre Dateien an und klicken Sie auf **Backup** ❷.



Wenn Sie keinen oder einen nicht erreichbaren Sicherungspfad eingeben, wird eine Fehlermeldung angezeigt.

Wenn die vorhandenen Netzlaufwerke in der Auswahl nicht angezeigt werden, prüfen Sie Ihre IT-Rechte bzw. das Laufwerk Mapping. Wenden Sie sich in diesem Fall an ihren IT-Support.



Speichern Sie die Sicherungsdaten nicht am Anlagenrechner bzw. Anlagenlaufwerk, sondern auf einem externen Datenspeicher. Dadurch sind im Schadensfall des Anlagenrechners die Backup Daten nicht betroffen.

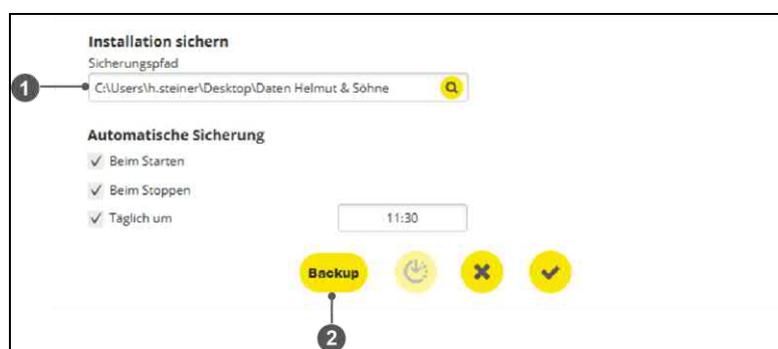


Abbildung 127: Manuelles Backup – Installation sichern

Ein Backup ist jederzeit bei laufendem Betrieb der Anlage möglich.

» 3. Schritt:

Die Sicherung läuft und es wird ein Fortschrittsbalken angezeigt.

Klicken Sie – wenn die Sicherung fertig ist – auf das Symbol **Bestätigen** ①. Sie kommen wieder auf die Anlagenseite des Xesar-Installation Managers.



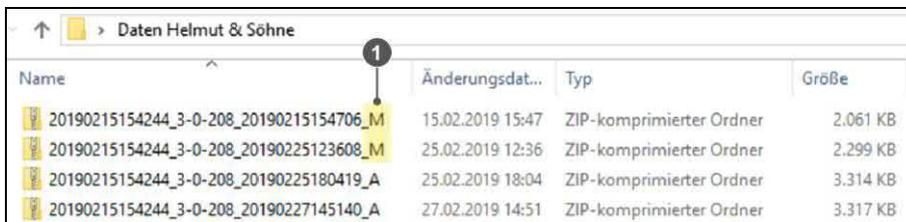
Abbildung 128: Manuelles Backup – Sicherungsprogramm läuft



Abbildung 129: Manuelles Backup – Sicherungsvorgang abgeschlossen

Die manuellen Backup-Daten liegen im Ordner, den Sie als Sicherungspfad angegeben haben. Sicherungsdateien von manuellen Backups sind mit einem **M**

am Dateinamenende ❶ gekennzeichnet. Es bleiben alle manuellen Backups gespeichert.



Name	Änderungsdat...	Typ	Größe
20190215154244_3-0-208_20190215154706_M	15.02.2019 15:47	ZIP-komprimierter Ordner	2.061 KB
20190215154244_3-0-208_20190225123608_M	25.02.2019 12:36	ZIP-komprimierter Ordner	2.299 KB
20190215154244_3-0-208_20190225180419_A	25.02.2019 18:04	ZIP-komprimierter Ordner	3.314 KB
20190215154244_3-0-208_20190227145140_A	27.02.2019 14:51	ZIP-komprimierter Ordner	3.317 KB

Abbildung 130: Manuelles Backup

6.2 Automatisches Backup

Im Xesar-Installation Manager sind auch automatische Backups möglich. Dazu wählen Sie auf der Einstellungsseite der Anlage unter **Automatische Sicherung** eine oder mehrere Optionen.

Für automatische Backups stehen folgende Varianten zur Verfügung:

Beim Starten ❶: Beim Starten der Anlage

Beim Stoppen ❷: Beim Stoppen der Anlage

Täglich um ❸: Zum eingestellten Zeitpunkt (die Uhrzeit ist frei wählbar ❹)



Abbildung 131: Automatisches Backup



Das Backup beim Starten und Stoppen der Anlage ist nur mit gesteckter und ausgewählter AdminCard möglich

Berücksichtigen Sie bei der Auswahl des Zeitpunktes für die automatische Sicherung: Das Backup zu einer definierten Uhrzeit ist nur möglich, wenn die Anlage und der Xesar-Installation Manager laufen.

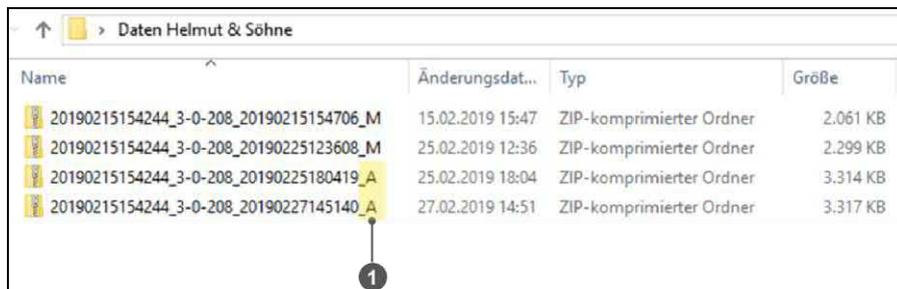
Der Admin-PC darf nicht in den Standby-Modus gehen, wenn automatische Backups durchgeführt werden sollen. Nach dem Standby-Mode muss der Xesar-Installation Manager neu gestartet werden.

6.3 Backup Files

Die manuellen Backup-Daten liegen im Ordner, den Sie als Sicherungspfad angegeben haben. Sicherungsdateien eines automatischen Backups sind mit einem **A** am Dateinamende ¹ gekennzeichnet.



Es bleibt pro Tag nur ein (das letzte) automatische Backup gespeichert. Generell bleiben nur die letzten drei automatischen Backups gespeichert.

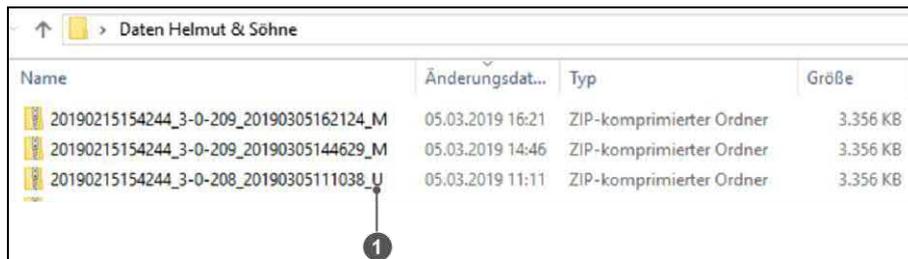


Name	Änderungsdat...	Typ	Größe
20190215154244_3-0-208_20190215154706_M	15.02.2019 15:47	ZIP-komprimierter Ordner	2.061 KB
20190215154244_3-0-208_20190225123608_M	25.02.2019 12:36	ZIP-komprimierter Ordner	2.299 KB
20190215154244_3-0-208_20190225180419_A	25.02.2019 18:04	ZIP-komprimierter Ordner	3.314 KB
20190215154244_3-0-208_20190227145140_A	27.02.2019 14:51	ZIP-komprimierter Ordner	3.317 KB

Abbildung 132: Backup Files



Vor einem Software-Update wird automatisch ein Backup durchgeführt. Diese automatische Backup-Daten liegen im Ordner, den Sie als Sicherungspfad angegeben haben. Sicherungsdateien eines Software-Updates sind mit einem **U** am Dateinamende ¹ gekennzeichnet



Name	Änderungsdat...	Typ	Größe
20190215154244_3-0-209_20190305162124_M	05.03.2019 16:21	ZIP-komprimierter Ordner	3.356 KB
20190215154244_3-0-209_20190305144629_M	05.03.2019 14:46	ZIP-komprimierter Ordner	3.356 KB
20190215154244_3-0-208_20190305111038_U	05.03.2019 11:11	ZIP-komprimierter Ordner	3.356 KB

Abbildung 133: Backup Files

6.4 Restore

Im Falle eines technischen Fehlers oder bei einem Wechsel der Hardware (PC) muss die Xesar-Software neu installiert werden.



Erstellen Sie vor einem Hardware zur Sicherung Ihrer Daten ein Backup.
Zur Wiederherstellung der Anlage wird die letzte Backup-Datei Ihrer Anlagendaten benötigt.



Erstellen Sie regelmäßige Backups von ihrer Xesar-Anlage.
Nutzen Sie dazu die Möglichkeit der automatischen Backups.
Besonders nach umfangreichen Änderungen erstellen Sie zumindest ein manuelles Backup.

Alle Änderungen, die Sie nach einem Backup durchführen und nicht sichern, können beim Restore nicht wieder hergestellt werden. Diese Änderungen müssen noch einmal vorgenommen werden.

Nach Restore eines Backups (auf demselben Rechner) oder Migration (auf einen anderen Rechner) muss in den Einstellungen der Xesar-Software die IP-Adresse des Servers kontrolliert bzw. korrigiert werden.

Wechsel der Anlagen-Hardware (PC)

» 1. Schritt:

Anlagen beenden

Wählen sie im Xesar-Installation Manager die Anlage aus.

Klicken Sie auf das Symbol **Beenden** (die Anlage ist beendet, wenn das Symbol ☹ angezeigt wird).


SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden
Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

» **2. Schritt:**

Anlage entfernen

Wählen Sie die Anlage aus und klicken Sie auf das Symbol **Entfernen** ①.

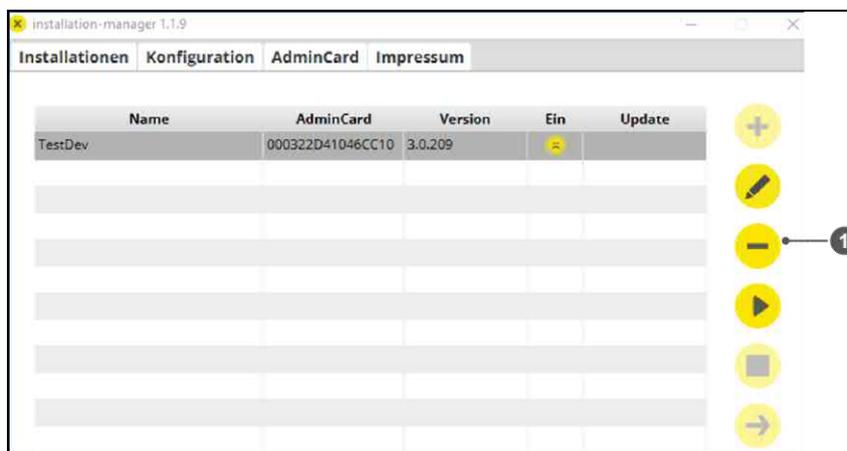


Abbildung 134: Anlage entfernen

Bestätigen Sie den folgenden Warnhinweis



Abbildung 135: Meldung – Installation wird entfernt

Wenn die Anlagendaten gelöscht wurden, erhalten Sie eine entsprechende Meldung.

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

» **3. Schritt:**

Installieren Sie den Xesar-Installation Manager neu und starten Sie den Xesar-Installation Manager.

Stecken Sie die Admin-Card der bestehenden Anlage in die Codierstation. Wählen Sie die kontaktbehaftete Leseinheit der Codierstation. Klicken Sie auf das Symbol **Laden** ①, um die AdminCard aufzuladen.

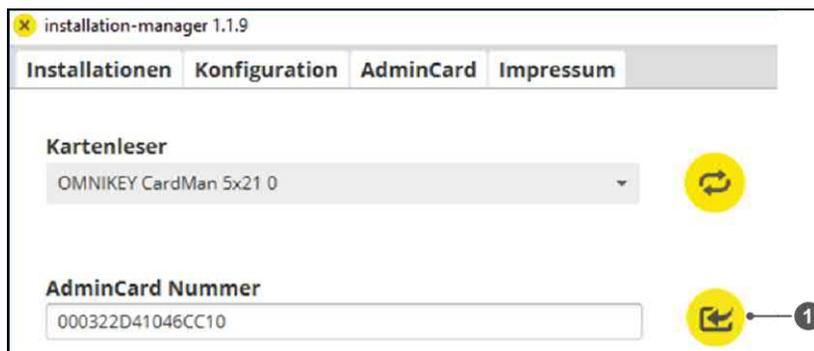


Abbildung 136: AdminCard Nummer Anzeige

Die AdminCard-Nummer wird angezeigt.

» **4. Schritt:**

Klicken Sie auf das Symbol **Hinzufügen** ①, um eine neue Anlage hinzuzufügen.

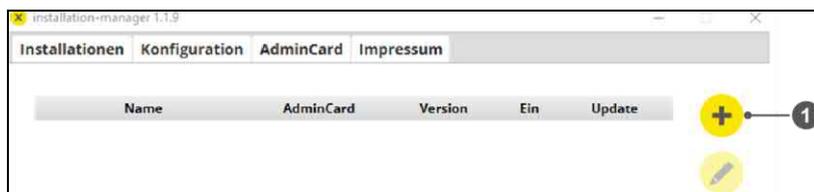


Abbildung 137: Restore



Die neue Anlage muss dieselbe Xesar-Software Version des Backup-Files haben. Gegebenenfalls muss im Xesar-Installation Manager für die Neuinstallation des Backups eine ältere Version aus der Versionsauswahl (Registry) gewählt werden. Das Xesar-Software Update kann nach abgeschlossener Backup-Installation erfolgen. Die Backupversion ist im Backup-Dateinamen beschrieben.

Folgende Informationen sind im Backup-Dateinamen beschrieben:

- Interner Anlagenname ①
- Backup-Software Version (z. B. 3.0 Version 207) ②
- Datum und Uhrzeit des Backups ③
- Backup-Art (**M**anuell, **A**utomatisch, automatisch vor **U**ppdate) ④

	20190122163121_3-0-207_20190124173132_M	24.01.2019 17:31
	20190122163121_3-0-207_20190127113002_A	27.01.2019 11:30
	20190122163121_3-0-207_20190128113002_A	28.01.2019 11:30
	20190122163121_3-0-207_20190129113637_A	29.01.2019 11:37

①
②
③
④

Abbildung 138: Restore

» 5. Schritt:

Tragen Sie die Anlageneinstellungen der neuen Anlage in die entsprechenden Felder ein.

- Name der Anlage ①
- Pfad zur letztgültigen Backup-Datei, die installiert werden soll ②
- neuer Pfad für die zukünftige Backups ③
- Automatische Backup Einstellungen ④
 - Beim Starten: Beim Starten der Anlage
 - Beim Stoppen: Beim Stoppen der Anlage
 - Täglich um: Zum eingestellten Zeitpunkt (Uhrzeit frei wählbar)

Klicken Sie auf das Symbol **Bestätigen** ⑥

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

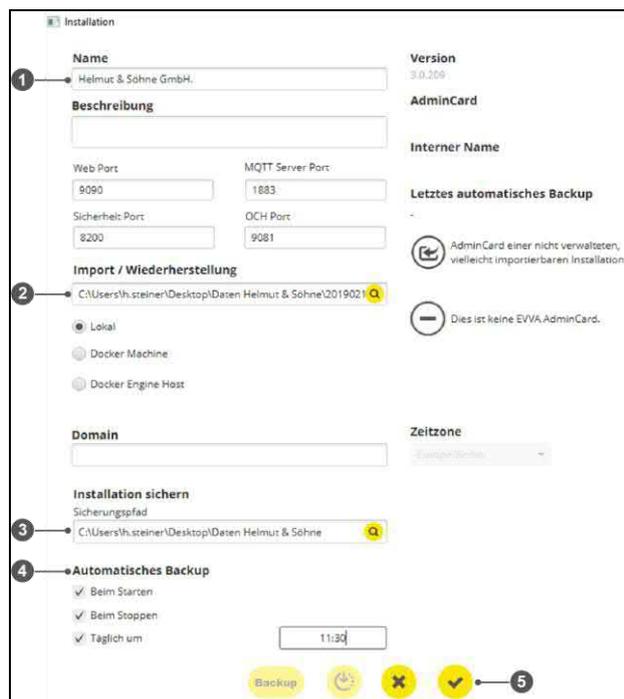


Abbildung 139: Restore

Folgende Anzeigen geben den Fortschrittsstatus an

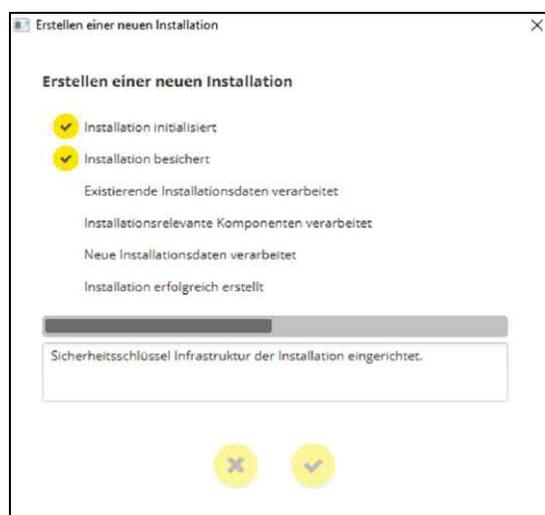


Abbildung 140: Restore



Abbildung 141: Restore

» **6. Schritt:**

Anlage starten

Klicken Sie auf das Symbol **Bestätigen**, wenn die Anlage erfolgreich erstellt wurde.

Wechsel Sie zum Xesar-Installation Manager, wählen Sie auf der Seite **Installationen** die Anlage aus und starten Sie die Anlage.

Damit ist die Anlage, basierend auf dem Stand der verwendeten Backup-Datei wiederhergestellt (restored).


SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

7 Inbetriebnahme Xesar-Software

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

Abbildung 142: Schritt für Schritt-Inbetriebnahme

7.1 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 **xls**. Alle Listen können als .csv- oder .xls-Datei exportiert und gedruckt werden. Als Dateiersprung 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.

7.2 Einstellungen



Abbildung 143: Kachel Einstellungen

7.2.1 Sicherheitseinstellungen



Abbildung 144: Sicherheitseinstellungen

7.2.2 Gültigkeits- und Berechtigungszeitraum der Identmedien

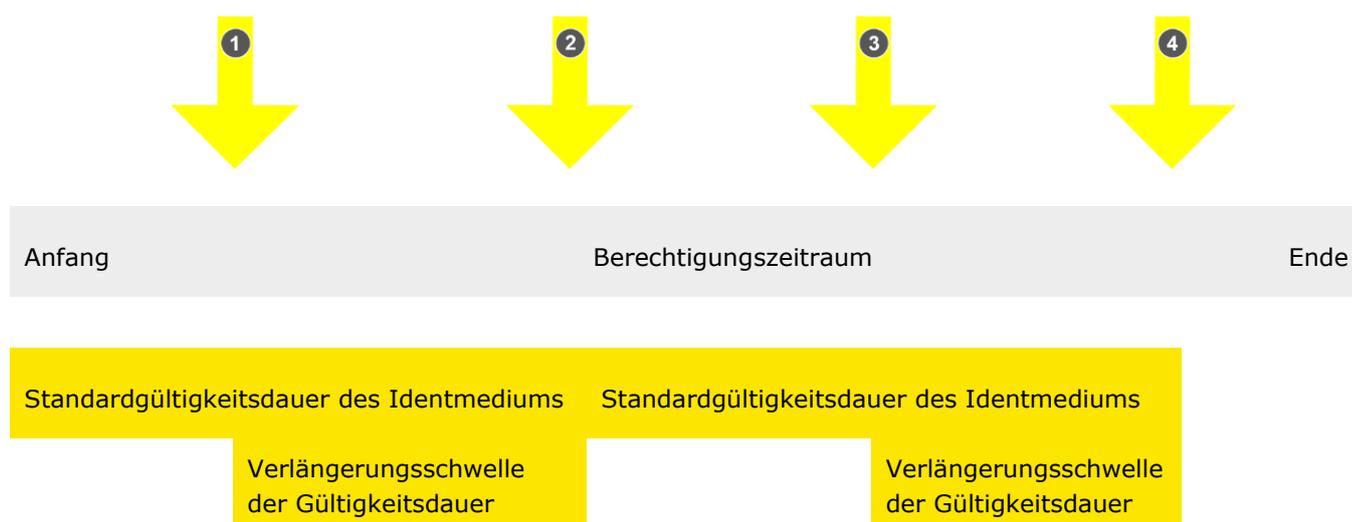


Abbildung 145: Gültigkeits- und Berechtigungszeitraum

- ① Frühestmögliches Update
- ② Spätestmögliches Update
- ③ Frühestmögliches Update
- ④ Spätestmögliches Update

Standardgültigkeitsdauer des Identmediums:

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

Die Standardgültigkeitsdauer kann bei Ausgabe von Identmedien individuell eingestellt werden.

Wenn die Standardgültigkeitsdauer abgelaufen ist wird das Identmedium ungültig und muss gegebenenfalls an der Codierstation oder am Xesar-Online Wandler aktualisiert werden.

Je kürzer die Standardgültigkeitsdauer ist, desto sicherer ist die Anlage, da das Identmedium 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 Identmediums an der Codierstation oder am Xesar-Online Wandler verlängert wird.

Standardberechtigungsdauer von Ersatz-Identmedien:

Die Standardberechtigungsdauer von Ersatz-Identmedien beträgt laut Systemvoreinstellung 72 Stunden. Die Standardberechtigungsdauer kann bei der Ausgabe von Ersatz-Identmedien individuell eingestellt werden (siehe Kapitel 7.11 Identmedien).

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.

7.2.3 Systemeinstellungen

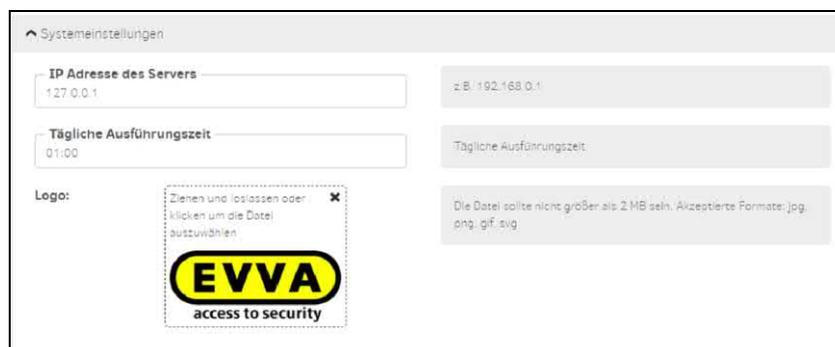


Abbildung 146: Systemeinstellungen

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 weitere Konfigurationseinstellungen des Xesar-Online Wandlesers mit der Xesar-Software (Backend) verwendet.



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

Logo:

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

Maximale Dateigröße: 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 datenschutzrechtliche Anforderungen Ihres Unternehmens.



Abbildung 147: Einstellungen zum Personenbezug

Es gibt 3 Datenspeichereinstellungen für Personen und Einbauorte:

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



Abbildung 148: Standardwert für Einbauorte (Personenbezug)

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



Einstellungen für das Programmiergerät:

Aus sicherheitstechnischen Gründen ist die Benutzung des Xesar-Tablets für anlagenrelevante Wartungsaufgaben mit einem PIN-Code geschützt.



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



Abbildung 149: Einstellungen für das Programmiergerät (Xesar-Tablet)

7.3 Benutzergruppen

In den Benutzergruppen werden die Berechtigungen für Benutzer definiert.



Abbildung 150: Kachel Benutzergruppen

Benutzer verwalten die Xesar-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.

Xesar > Benutzergruppen

+ ↻

Zeige Einträge 1 - 5 von 5 (5 gesamt) ⚙

▲ Name	↕ Beschreibung	↕ Anzahl aktiver Benutzer	↕ Anzahl nicht aktiver Benutzer
Installationsverwalter		2	0
Wartungstechniker		2	0
Partitionsverwalter		2	0
Empfang		2	0
Systemadministrator		3	0

Abbildung 151: Vordefinierte Benutzergruppen

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:

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

Xesar > Benutzergruppen > Installationsverwalter

^ Benutzergruppe

Name *
Installationsverwalter

Beschreibung

^ Berechtigungen

▼ Allgemein Lesen auswählen Alle auswählen

▼ Personen Lesen auswählen Alle auswählen

▼ Einbauorte Lesen auswählen Alle auswählen

▼ Bereiche Lesen auswählen Alle auswählen

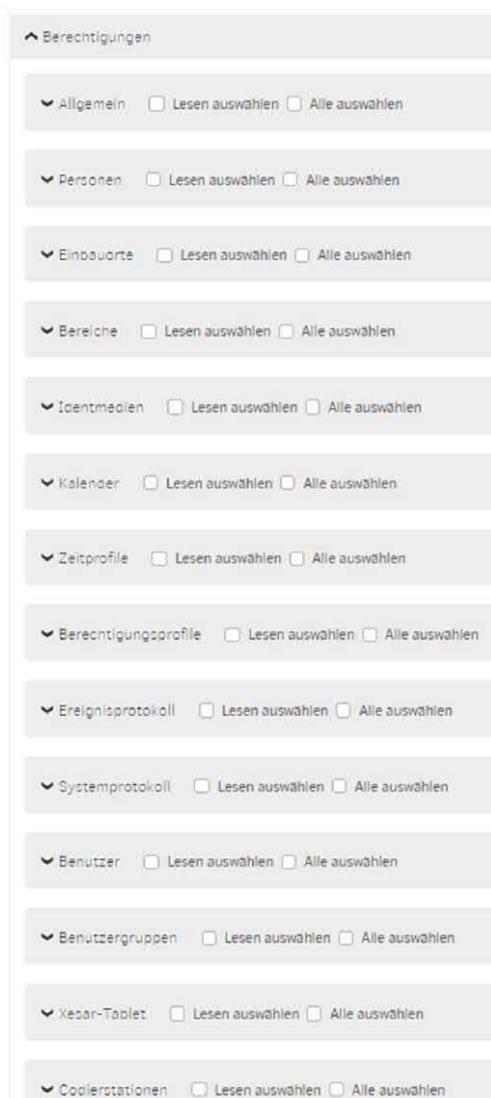
Abbildung 152: Benutzergruppe Installationsverwalter



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 Xesar-Dashboard gruppiert.

In jeder Berechtigungsgruppe werden folgende Berechtigungen definiert:

- nur Leseberechtigungen
- alle Berechtigungen ausgewählt werden.

Abbildung 153: Benutzergruppen
Berechtigungen

Beispiel Individuelle Benutzergruppe – Empfang Haupteingang mit Basis Benutzergruppe Empfang ① und zusätzlichen Lese- und Bearbeitungsrechten für Personeneinstellungen:

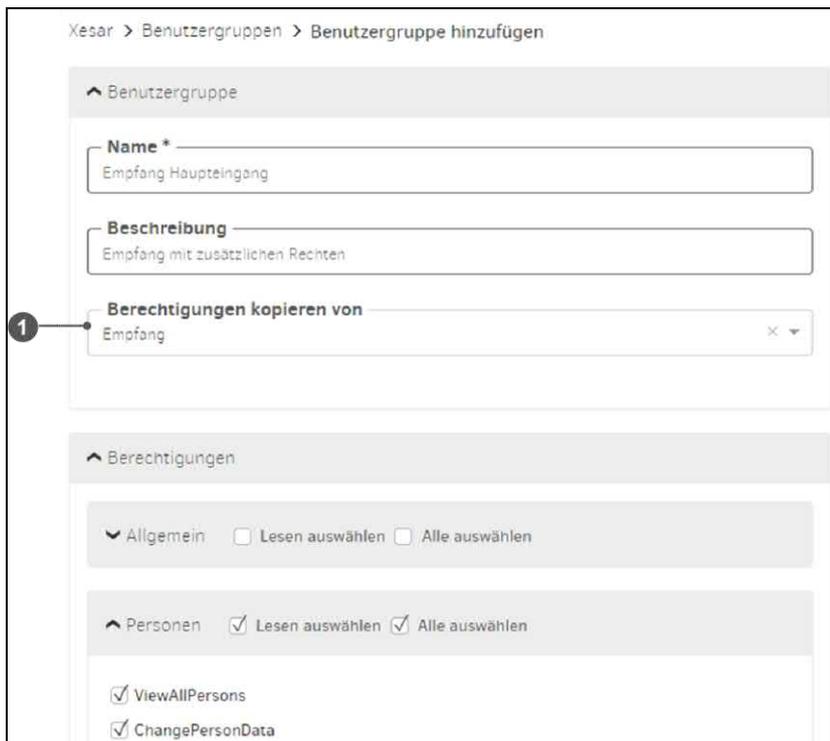


Abbildung 154: Benutzergruppe Empfang Haupteingang



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 Identmedien zuweisen. Die Benutzer der anderen Benutzergruppen dürfen zusätzlich die Berechtigungsprofile Chef und Assistentin, Feuerwehr- sowie Master Key-Berechtigungsprofil einem Identmedium zuweisen.

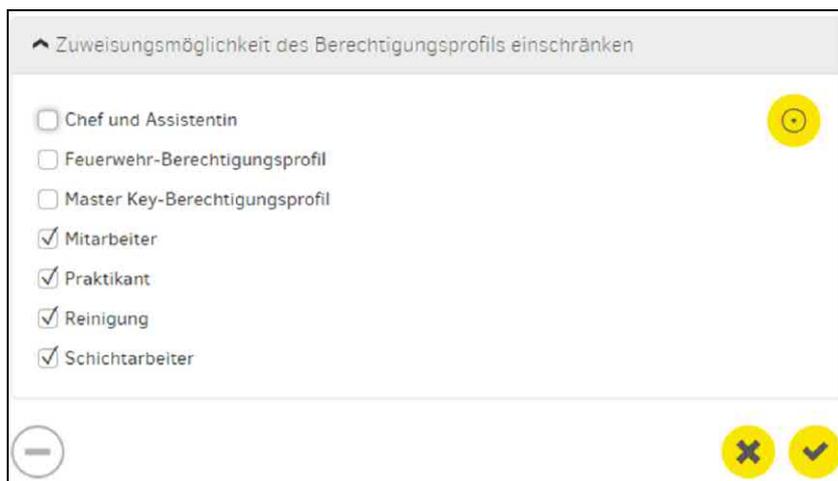


Abbildung 155: Beispiel Zuweisungsmöglichkeit der Berechtigungsprofile einschränken

7.4 Benutzer

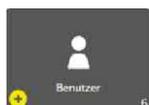


Abbildung 156: Kachel Benutzer

Benutzer verwalten die Xesar-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 Xesar-Anlage mit Ihnen zugewiesenen Identmedien 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

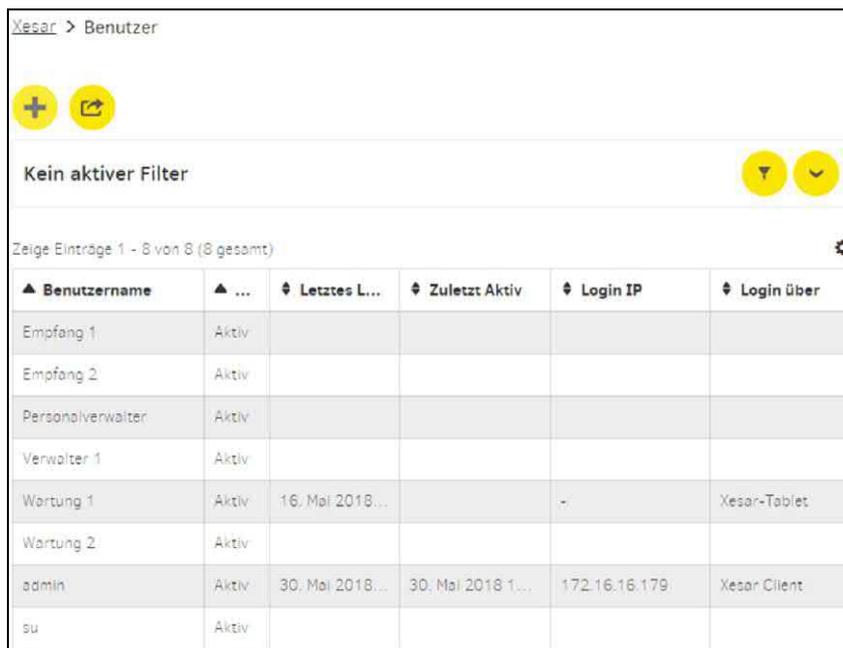


Abbildung 157: Benutzergruppen

- **admin**
hat alle Berechtigungen



Abbildung 158: Adminrechte



Xesar > Benutzer

Kein aktiver Filter

Zeige Einträge 1 - 8 von 8 (8 gesamt)

▲ Benutzername	▲ ...	⬇ Letztes L...	⬇ Zuletzt Aktiv	⬇ Login IP	⬇ Login über
Empfang 1	Aktiv				
Empfang 2	Aktiv				
Personalverwalter	Aktiv				
Verwalter 1	Aktiv				
Wartung 1	Aktiv	16. Mai 2018...		-	Xesar-Tablet
Wartung 2	Aktiv				
admin	Aktiv	30. Mai 2018...	30. Mai 2018 1...	172.16.16.179	Xesar Client
su	Aktiv				

Abbildung 159: Benutzerübersicht

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

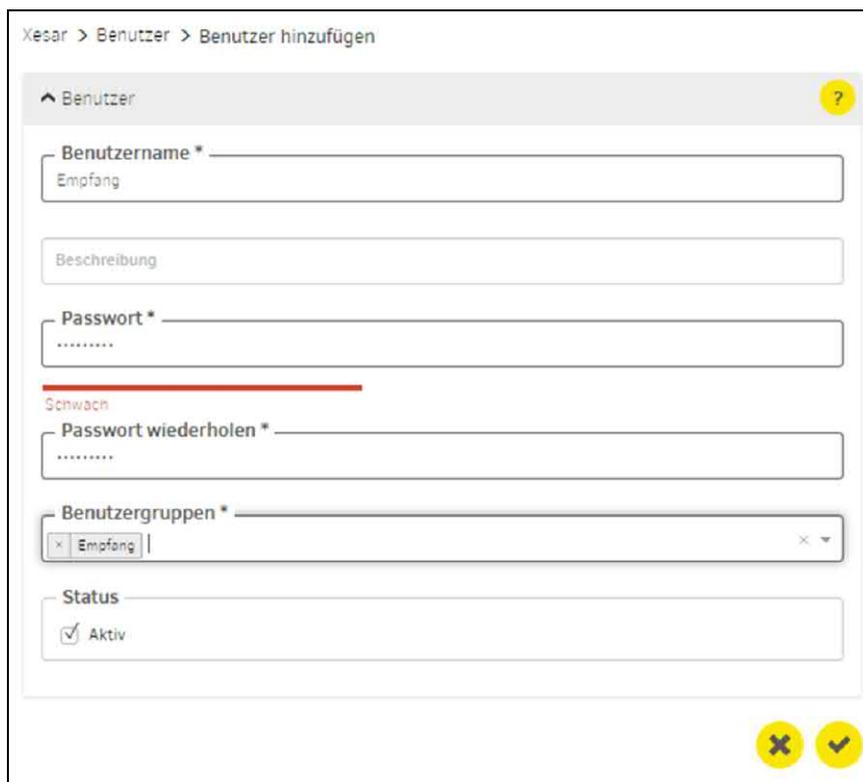
(Diese Feld wird erst nach dem ersten Speichern angezeigt)

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.



Xesar > Benutzer > Benutzer hinzufügen

Benutzer

Benutzername *
Empfang

Beschreibung

Passwort *
.....
Schwach

Passwort wiederholen *
.....

Benutzergruppen *
Empfang

Status
 Aktiv

Abbildung 160: Neuer Benutzer

Konfiguration herunterladen

Das jeweilige Benutzerzertifikat (Konfiguration) wird heruntergeladen. Das

Benutzerzertifikat wird für eine gesicherte Drittschnittstellen-Aktionen (z. B. Personen-Datenimport über die Drittschnittstelle) benötigt.



Abbildung 161: Konfiguration herunterladen

7.5 Kalender



Abbildung 162: Kachel 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.



Abbildung 163: Anzeige der Kalender

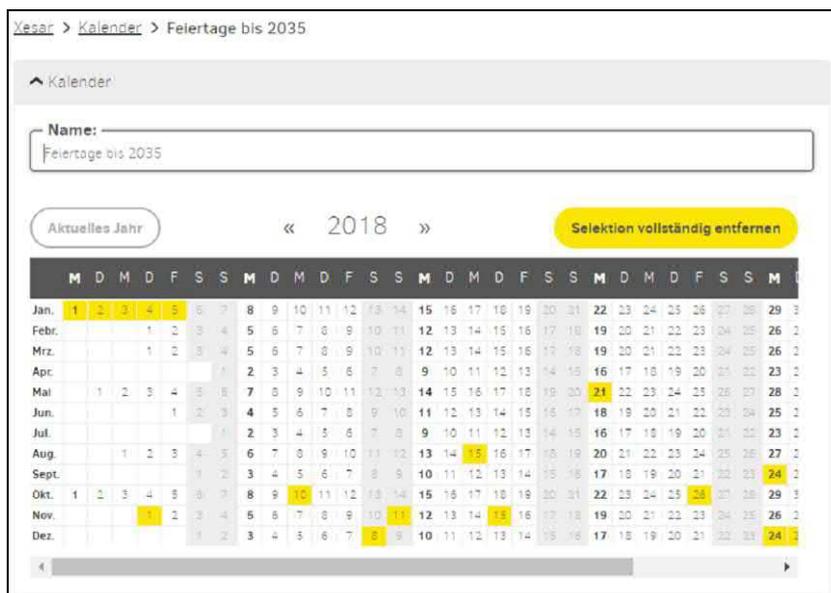


Abbildung 164: Kalender

Kalender importieren:

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



Abbildung 165: Kalender importieren



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

7.6 Zeitprofile



Abbildung 166: Kachel Zeitprofile

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

Wird bei der Erstellung eines Identmediums kein Zeitprofil verwendet, gilt für dieses Identmedium keine Zutrittszeiteinschränkung – das Identmedium 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 Identmedium.

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 Identmedium 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 Identmedium 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 Identmedium.

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 Identmedium 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 Identmedium 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 Identmedium 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 Identmediums an der Xesar-Zutrittskomponente aktiviert. Sie erhalten eine entsprechende optische und akustische Bestätigung (siehe 2.3 Ereignissignalisierung).

Der Manual Office Mode wird automatisch zum definierten Schließzeitpunkt beendet oder manuell, durch erneutes, zweimaliges Anhalten eines berechtigten Identmediums an der Xesar-Zutrittskomponente. Sie erhalten eine entsprechende optische und akustische Bestätigung (siehe 2.3 Ereignissignalisierung).

Manual Office Mode und Shop Mode aktivieren:

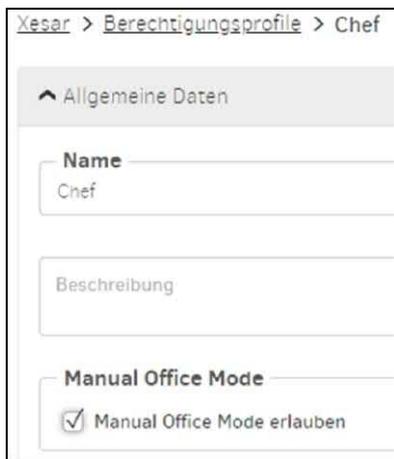
Öffnen Sie Xesar > Einbauorte > Haupteingang



The screenshot shows a configuration window with two sections. The first section is titled 'Manual Office Mode' and contains a checked checkbox labeled 'Manual Office Mode erlauben'. The second section is titled 'Shop Mode' and contains a checked checkbox labeled 'Shop Mode aktivieren'.

Abbildung 167: Manual Office Mode / Shop Mode aktivieren

Öffnen Sie Xesar > Berechtigungsprofile > Benutzer



The screenshot shows the configuration page for a user profile named 'Chef'. The breadcrumb path is 'Xesar > Berechtigungsprofile > Chef'. Under the 'Allgemeine Daten' section, the 'Name' field contains 'Chef' and the 'Beschreibung' field is empty. In the 'Manual Office Mode' section, the checkbox 'Manual Office Mode erlauben' is checked.

Abbildung 168: Manual Office Mode aktivieren


SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

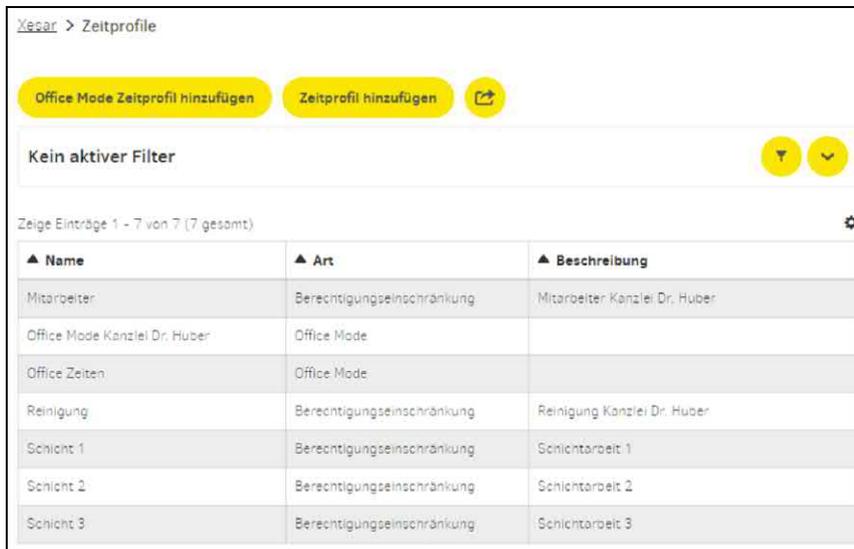
Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

Ansicht Zeitprofile:



Xesar > Zeitprofile

Office Mode Zeitprofil hinzufügen Zeitprofil hinzufügen 

Kein aktiver Filter  

Zeige Einträge 1 - 7 von 7 (7 gesamt) 

Name	Art	Beschreibung
Mitarbeiter	Berechtigungseinschränkung	Mitarbeiter Kanzlei Dr. Huber
Office Mode Kanzlei Dr. Huber	Office Mode	
Office Zeiten	Office Mode	
Reinigung	Berechtigungseinschränkung	Reinigung Kanzlei Dr. Huber
Schicht 1	Berechtigungseinschränkung	Schichtarbeit 1
Schicht 2	Berechtigungseinschränkung	Schichtarbeit 2
Schicht 3	Berechtigungseinschränkung	Schichtarbeit 3

Abbildung 169: Ansicht der Zeitprofile

7.6.1 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.



Abbildung 170: Fehlermeldung Zeitfenster

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.

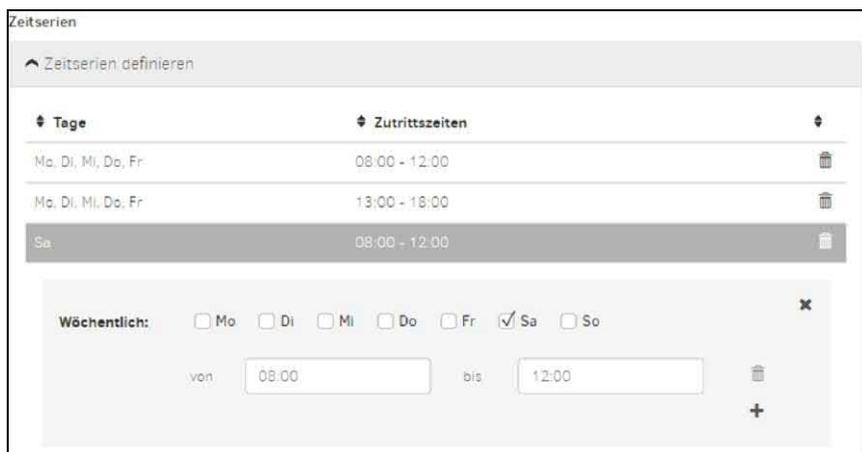


Abbildung 171: Manual Office Mode Zeitserienausnahmen:

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.



Abbildung 172: Zeitserienausnahme

Zeitpunktserien:

Zeitpunktserien 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 Identmedien durch zweimaliges Anhalten an der Xesar-Zutrittskomponente aktiviert werden.



Es sind maximal 35 Zeitpunktserien möglich.

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

Zeitpunktserien		
^ Zeitpunktserien definieren		
⚙ Tage	⚙ Schließzeitpunkt	⚙
Mo, Di, Mi, Do, Fr	20:00	🗑

Abbildung 173: Zeitpunktserie

Ausnahme der Zeitpunktserien:

Für Sonder- oder Feiertage kann der Schließzeitpunkt geändert werden.

^ Ausnahmen zu den Zeitpunktserien		
⚙ Tage	⚙ Schließzeitpunkt	
Feiertage bis 2035	13:00	

Abbildung 174: Ausnahmen zu den Zeitpunktserien

7.6.2 Zeitprofil hinzufügen

Zeitprofile können für Personen und Identmedien 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.

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

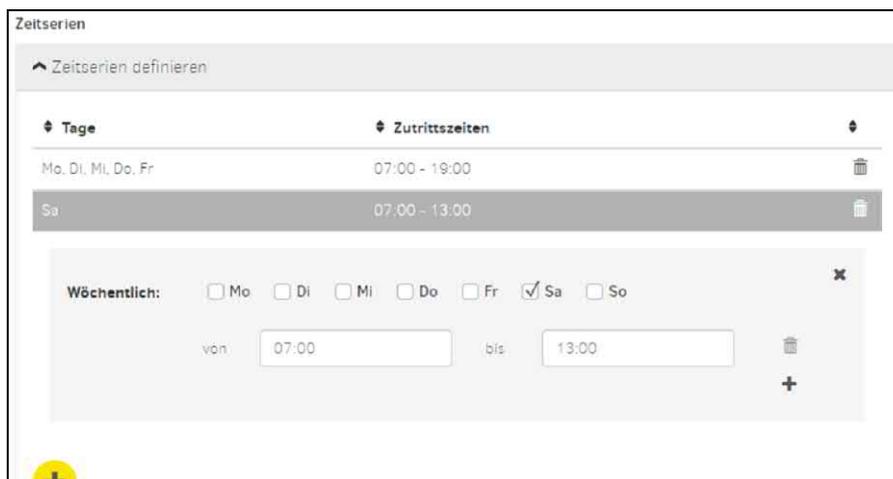


Abbildung 175: Zeitprofil hinzufügen

Zeitreienausnahmen:

Zeitreienausnahmen definieren Abweichungen von Zeitreihen, 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.



Abbildung 176: Zeitserienausnahmen

7.7 Einbauorte



Abbildung 177: Kachel Einbauorte

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

ID	Name	Art	Komponententyp	Zustand im Lebenszyklus	Letzte Zustandsänderung	Batteriewarnung	Wartungsaufgabe
BB01	Büro Dr. Huber	Isolierte Tür		Zum Hinzufügen vorbereitet	2018-06-17T17:39:23+02		EVVA-Komponente hinzufügen
WLS1	Hauptingang Kitzle's Dr. Huber	Automatische Schließanlage		Zum Hinzufügen vorbereitet	2018-06-17T17:38:37+02		EVVA-Komponente hinzufügen
EG-002	Reparaturgang Parkplatz	Tür		Zum Hinzufügen vorbereitet	2018-04-30T10:28:11+02		EVVA-Komponente hinzufügen
EG-003	Garage 01	Tür		Zum Hinzufügen vorbereitet	2018-04-30T10:28:03+02		EVVA-Komponente hinzufügen

Abbildung 178: Anzeige Einbauorte

7.7.1 Einbauort hinzufügen:

Wählen Sie die gewünschte Xesar-Zutrittskomponente aus.

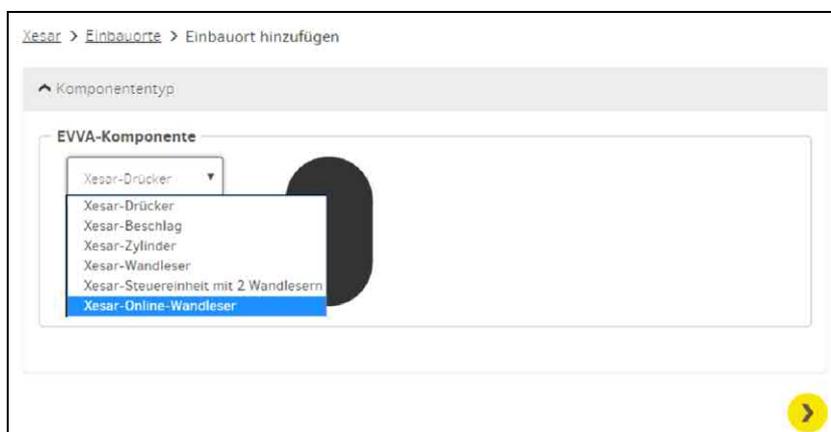


Abbildung 179: Einbauort hinzufügen

7.7.2 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. Zent-raler Zugang, Fluchtweg zu Sammelplatz Wienerbergstraße, ...

Art Einbauort:

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

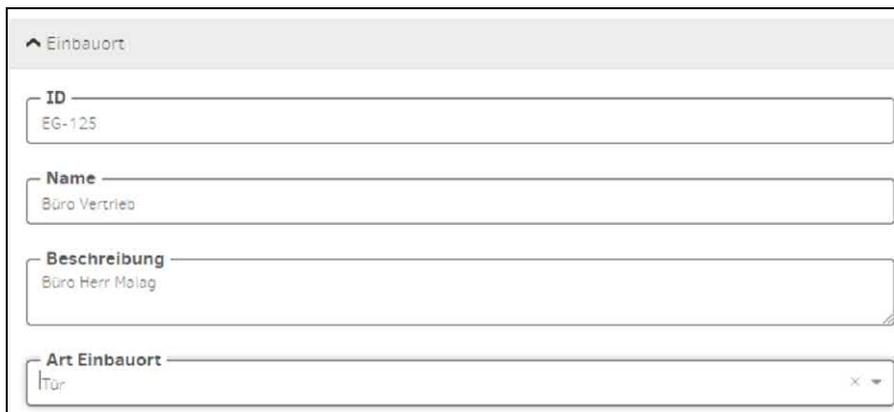


Abbildung 180: Einbauort beschreiben

Freigabedauer:

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

Die Zuordnung der Freigabedauer zur Person bzw. dem Identmedium erfolgt bei den Personen- und Identmedieneinstellungen.



Abbildung 181: Freigabedauer

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



Abbildung 182: Zeitprofil (Einbauort)



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

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

7.8 Bereiche



Abbildung 183: Kachel 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.

Xesar > Bereiche

Kein aktiver Filter

Zeige Einträge 1 - 4 von 4 (4 gesamt)

Name	Beschreibung	Anzahl Einbauorte
Büros	alle Büros	2
Spinde	alle Spinde	2
Aussetztüren	alle Aussetztüren	3
Installation		7

Abbildung 184: Ansicht Bereiche

Beispiel Anzeige Bereich Büros:

Pflichtfelder sind mit * gekennzeichnet.

Name:

Name des Bereichs

Beschreibung:

Ergänzende Informationen zum Namen

Einbauorte:

Anzeige der ausgewählten Einbauorte

Bereich

Name: Büros

Beschreibung: Alle Büros - Eingänge

Einbauorte

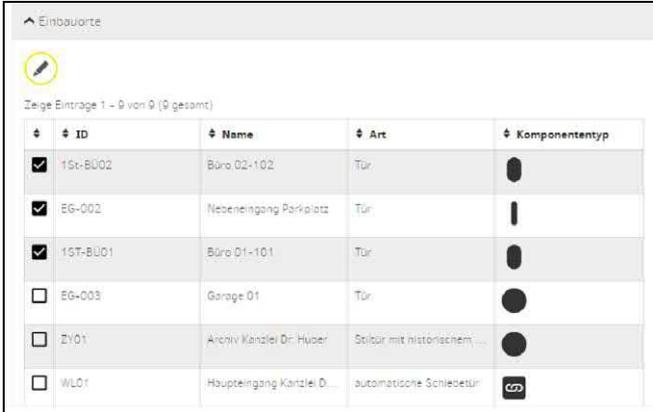
Zeige Einträge 1 - 3 von 3 (3 gesamt)

ID	Name	Art	Komponententyp
1St-BU02	Büro 02-102	Tür	
EG-002	Nebeneingang Parkplatz	Tür	
1ST-BU01	Büro 01-101	Tür	

Abbildung 185: Anzeige Bereich - Büros

Auswahl von Einbauorten:

Wählen Sie die Einbauorte für den Bereich aus, indem Sie in der ersten Spalte das Feld aktivieren.



ID	Name	Art	Komponententyp
<input checked="" type="checkbox"/> 1ST-BU02	Büro 02-102	Tür	
<input checked="" type="checkbox"/> EG-002	Nebeneingang Parkplatz	Tür	
<input checked="" type="checkbox"/> 1ST-BU01	Büro 01-101	Tür	
<input type="checkbox"/> EG-003	Garage 01	Tür	
<input type="checkbox"/> ZV01	Archiv Kanzlei Dr. Huber	Schleuse mit historischem...	
<input type="checkbox"/> WLD01	Haupteingang Kanzlei D...	automatische Schiebetür	

Abbildung 186: Auswahl von Einbauorten

7.9 Berechtigungsprofile

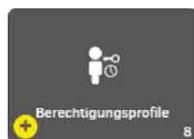


Abbildung 187: Kachel Berechtigungsprofile

Berechtigungsprofile beschreiben räumliche und zeitliche Zutrittsbeschränkungen für Identmedien. Diese Identmedien können Personen zugewiesen werden. Das heißt, eine Person mit einem Identmedium 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 Identmedien zugewiesen werden (z.B. allen Personen einer Abteilung mit gleichen Berechtigungen).

Jedem Identmedium kann nur ein Berechtigungsprofil zugewiesen werden. Zusätzlich zu diesem Berechtigungsprofil können jedem Identmedium 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**.

Xesar > Berechtigungsprofile

Kein aktiver Filter  

Zeige Einträge 1 - 7 von 7 (7 gesamt) 

↕ Name	↕ Beschreibung	▲ Status Berechtigungen
Handwerker	für Arbeiter der Fa. Baufix	Nein
Praktikant	für alle Praktikanten	Ja
Schichtarbeiter	für alle Schichtarbeiter der Spät-Schicht	Ja
Empfang	für alle Empfangs-Mitarbeiter	Ja
Mitarbeiter	für alle Verkaufsmitarbeiter	Ja
Chef und Assistentin	für Chef und Assistentin	Ja
Reinigung	für Mitarbeiter der Reinigungsfirma Sauber	Ja

Abbildung 188: Berechtigungsprofile

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. Ident-medien die Berechtigung, den manuellen Office Mode an den berechtigten Xesar-Zutrittskomponenten zu aktivieren.

Standard Zeitprofil:

Auswahl aus den Zeitprofilen



Für das Standard-Zeitprofil dürfen nur Zeitprofile mit maximal 12 Zeitfenstern verwendet werden.

Xesar > Berechtigungsprofile > Schichtarbeiter

^ Allgemeine Daten

Name
Schichtarbeiter

Beschreibung
für alle Schichtarbeiter der Spät-Schicht

Manual Office Mode
 Manual Office Mode erlauben

Standard Zeitprofil
Zeitprofil Schichtarbeiter x ▾

Das Standard Zeitprofil gilt auch für die Individualberechtigungen eines Identmediums.

Abbildung 189: Berechtigungsprofil Beispiel - Schichtarbeiter

Auswahl der Einbauorte:

Einbauorte



Zeige Einträge 1 - 7 von 7 (7 gesamt)

<input type="checkbox"/>	ID	Name	Art	Kompon...	Zeitprofil
<input checked="" type="checkbox"/>	HE-001	Haupteingang	elektrische ...		Zeitprofil Schichtarbeiter ▾
<input checked="" type="checkbox"/>	NE-001	Nebeneingang			Zeitprofil Schichtarbeiter ▾
<input type="checkbox"/>	BÜ-002	Büro Vertrieb	Glastür		Zeitprofil Schichtarbeiter ▾
<input type="checkbox"/>	BÜ-001	Chef Büro	Tür		Zeitprofil Schichtarbeiter ▾

Abbildung 190: Auswahl der Einbauorte

Zutritt zu ausgewählten Einbauorten:

Einbauorte



Zeige Einträge 1 - 2 von 2 (2 gesamt)

ID	Name	Art	Kompon...	Zeitprofil
HE-001	Haupteingang	elektrische S...		Zeitprofil Schichtarbeiter ▾
NE-001	Nebeneingang			Zeitprofil Schichtarbeiter ▾

Abbildung 191: Zutritt zu ausgewählten Einbauorten

7.10 Personen



Abbildung 192: Kachel Personen

Im Bereich Personen werden alle relevanten Informationen der in der Anlage berechtigten Personen definiert. Personen einer Anlage können ein oder mehrere Identmedien mit unterschiedlichen Berechtigungsprofilen zugewiesen werden. Personen können auch Benutzer mit entsprechenden Rechten (laut entsprechender Benutzergruppe) sein.

Anzeige Personenliste:

Nachname	Vorname	ID	Anzahl ausgegebener I...	Standardberechtigungsprofil	Ext...	Nicht aktuelle Identmedien
Aigner	Nico	NA035	4	Berechtigung Werkstätt 2	Ja	Nein
Angerer	Elisabeth	NA112	0	Berechtigung Werkstätt 2	Ja	Nein
Auer	Michael	NA030	0	Berechtigung Lager	Ja	Nein
Bauer	Lukas	NA003	0	Berechtigung Werkstätt 1	Ja	Nein
Baumann	Eva	NA110	0	Berechtigung Lager	Ja	Nein
Baumgartner	Benjamin	NA026	0	Berechtigung Lager	Ja	Nein
Berger	Leon	NA011	0	Berechtigung Werkstätt 1	Ja	Nein
Binder	Ben	NA032	0	Berechtigung Werkstätt 2	Ja	Nein
Brandstetter	Livia	NA117	0	Berechtigung Büro	Ja	Nein

Abbildung 193: Anzeigen Personenliste

Pflichtfelder sind mit * gekennzeichnet.

Vorname:

Vorname der Person

Nachname:

Nachname der Person

ID:

Kurzzeichen der Person, z.B. Initialen

Anzahl der ausgegebenen Identmedien:

Anzahl der zugewiesenen Identmedien für die Person

Standardberechtigungsprofil:

Auswahl aus den Berechtigungsprofilen; wird als Standardberechtigungsprofil auf das Identmedium geschrieben, das der Person zugewiesene 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 Identmedien:

Ja – Mindestens ein Identmedium der Person ist nicht aktuell und muss durch Anhalten am Xesar-Online Wandler oder Auflegen auf der Codierstation aktualisiert werden.

(Die Darstellung der Statuskachel **Identmedien nicht aktuell** am Xesar-Dashboard ist gelb.)

Nein – Alle Identmedien der Person sind aktuell; Anhalten am Xesar-Online Wandler oder Auflegen auf der Codierstation ist nicht notwendig.

7.10.1 Person hinzufügen

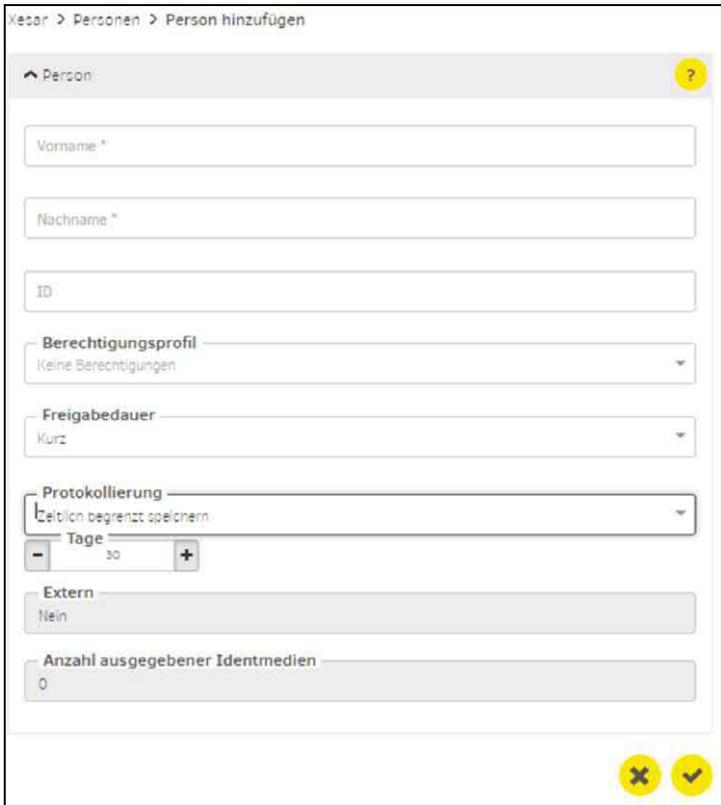


Abbildung 194: Person hinzufügen

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 Identmedium geschrieben, das der Person zugewiesene ist.

Freigabedauer:

Die Freigabedauer ist **Kurz** oder **Lang** und wird bei berechtigtem Zutritt an der Xesar-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 Identmedien:

Anzahl der zugewiesenen Identmedien für die Person



■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

7.11 Identmedien



Abbildung 195: Kachel Identmedien

Identmedien dienen zum Öffnen von Türen bei vorhandener Berechtigung sowie zum Transport von anlagenspezifischen Sicherheitsdaten zwischen den Xesar-Zutrittskomponenten und der Verwaltungssoftware über das virtuelle Netzwerk XVN (Xesar Virtuelles Netzwerk).

7.11.1 Neues Identmedium

Mit Auflegen eines neuen Xesar-Identmediums auf die Codierstation erscheint folgendes Eingabefeld:



Abbildung 196: Neues Identmedium

ID:

(Identifikator oder Kennzeichen ist kein Pflichtfeld)

Sie können dem Identmedium eine Identmedienbezeichnung (z.B. Hans Huber Garage, Besucher 1 oder Zimmer 23) geben.

Die Vergabe oder Änderung einer ID ist jederzeit in der Identmedium-Detailansicht in der Xesar Software möglich.



Das Kennzeichen eines Identmediums 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 Identmedien vergibt.

Nach Bestätigung erscheint eine weitere Seite mit folgenden Anzeige- und Eingabefeldern:

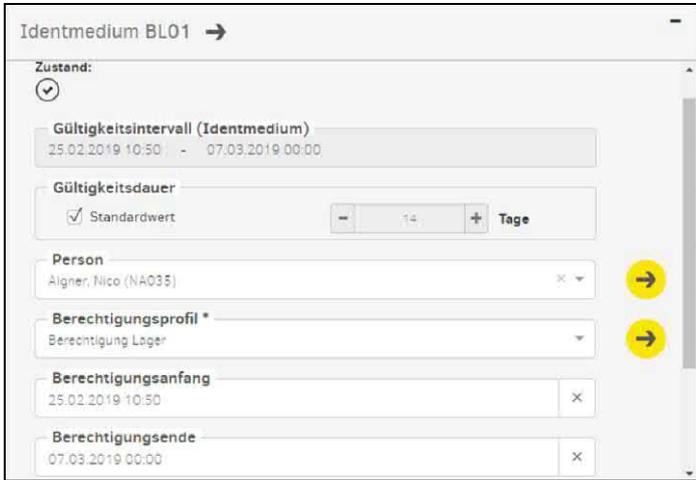


Abbildung 197: Identmedium zuweisen

Pflichtfelder sind mit * gekennzeichnet.

Zustand:

Aktuellen Zustand betreffend Gültigkeit und Aktualität.

Gültigkeitsintervall:

Auswahl des Zeitintervalls, bis das Identmedium wieder am Xesar-Online Wandler oder der Codierstation aktualisiert werden muss (Gültigkeit wird verlängert).

Gültigkeitsdauer:

Information des Zeitraums, für den das Identmedium gültig ist.

Standardwert:

Wird in den allgemeinen Sicherheitseinstellungen definiert.

Individuell:

Eingabe 1 Tag bis max. 7300 Tage (ca. 20 Jahre)

Person:

Das Identmedium kann einer angelegten Person zugewiesen werden. Einer Person können mehrere Medien zugewiesen werden.

Identmedium (Ersatzmedium):

Zum Erstellen eines Ersatzmediums wird hier das zu ersetzende Identmedium der oben ausgewählten Person mit seinem Berechtigungsprofil ausgewählt.

Berechtigungsprofil:

Auswahl des gewünschten Berechtigungsprofils

Berechtigungsanfang:

Zeitpunkt für Berechtigungsanfang des Identmediums. Der Zeitpunkt kann auch in der Zukunft liegen, z. B. bei Hotelbuchungen.

Berechtigungsende:

Der Zeitpunkt für Berechtigungs- und Gültigkeitsende des Identmediums (z. B. Praktikumsende).

Nach diesem Zeitpunkt kann die Gültigkeit des Identmediums nicht mehr verlängert werden.

Individuelle Berechtigungen:

Einem Identmedium 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.

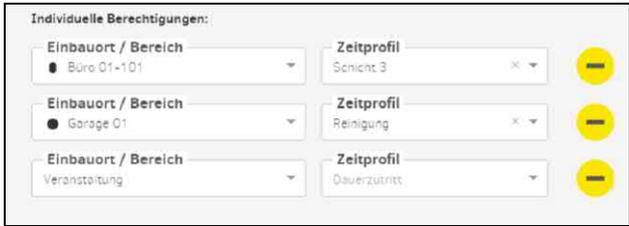


Abbildung 198: Individuelle Berechtigung

7.11.2 Vorhandenes Identmedium

Nach Auflegen eines bestehenden Identmediums auf die Codierstation wird folgendes Eingabefenster angezeigt:

Zustand des Identmediums:

#	Zustand	Visualisierung	Erklärung
1	Unsicher gesperrtes Identmedium		Es gibt noch unsere Einbauorte
2	Sicher gesperrtes Identmedium		Es gibt keine unsicheren Einbauorte mehr.
3	Unberechtigtes Identmedium		Das Identmedium hat keine Berechtigung
4	Aktuell gültig		

#	Zustand	Visualisierung	Erklärung
5	Aktuell ungültig		
6	Aktuell gültiges Identmedium, das bei Aktualisierung zu einem ungültigen Identmedium wird	 	
7	Aktuell ungültiges Identmedium, das bei Aktualisierung zu einem gültigen Identmedium wird	 	
8	Aktuell ungültiges Identmedium mit einem Gültigkeitsintervall auf dem Identmedium, das in der Zukunft liegt	 	
9	Deaktiviertes Identmedium		Das Medium wurde deaktiviert. Es gibt keine unsicheren Einbauorte mehr und der Kalender spielt keine Rolle mehr.

Tabelle 4: Zustand des Identmediums

Gültigkeitsintervall:

Auswahl des Zeitintervalls, bis das Identmedium wieder am Xesar-Online Wandler oder der Codierstation aktualisiert werden muss (Gültigkeit wird verlängert).

Gültigkeitsdauer:

Information des Zeitraums, für den das Identmedium gültig ist.

Standardwert:

Wird in den allgemeinen Sicherheitseinstellungen definiert.

Individuell:

Eingabe 1 Tag bis max. 7300 Tage (ca. 20 Jahre)

Person:

Person, der dieses Identmedium zugewiesen ist

Berechtigungsanfang:

Ab diesem Zeitpunkt ist das Identmedium berechtigt zum Berechtigungsupdate bzw. gültig

Berechtigungsende:

Ab diesem Zeitpunkt ist das Identmedium nicht mehr berechtigt zum Berechtigungsupdate bzw. nicht mehr gültig

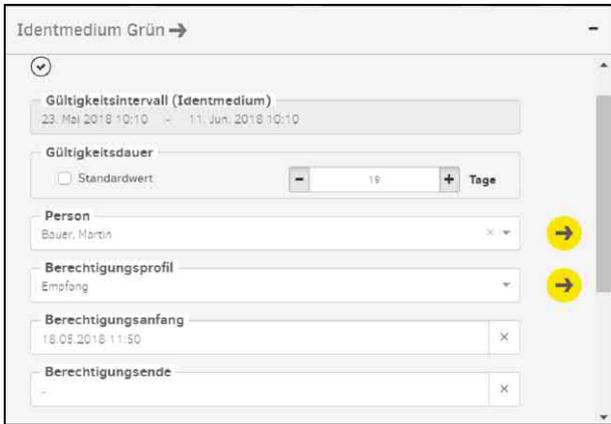


Abbildung 199: Identmedium

Individuelle Berechtigungen:

für 3 Einbauorte bzw. Bereiche können dem Identmedium 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 Identmedien von Mitarbeitern verwendet, die das Unternehmen verlassen.)



Identmedien können wiederverwendet werden.
Verwenden Sie daher für die Identmedien-ID keine personenbezogenen Daten.

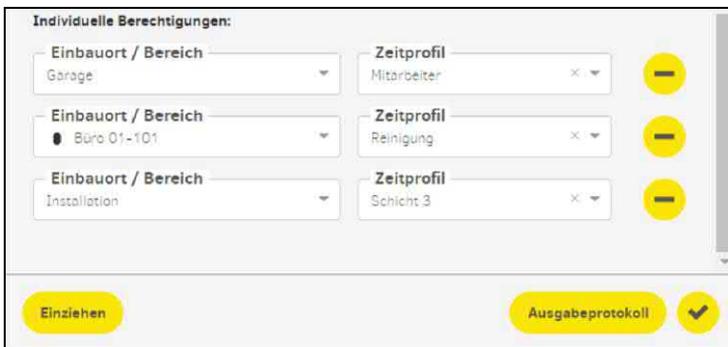


Abbildung 200: Identmedium – Individuelle Berechtigung

Ausgabeprotokoll:

Klicken Sie auf den Button **Ausgabeprotokoll**, wird ein Identmedienausgabeprotokoll mit allen relevanten Daten als Datei im .pdf-Format generiert. Die pdf-Datei kann ausgedruckt und bei der Übernahme des Identmediums vom Empfänger mit seiner Unterschrift bestätigt werden.



Erstellen Sie bei Änderungen der Berechtigungen ein neues Ausgabeprotokoll.

Xesar
Ausgabeprotokoll

Vorname der Person: Hübner
 Nachname der Person: Steiner
 ID Person: 1017
 ID Identmedium: Karte H52
 Freigabezeitraum: Kurz
 Protokollierung: Nicht speichern
 Zeitraum Protokollierung: ---
 Berechtigungszeitraum: 7. Jun. 2018 13:05 - 26. Jul. 2019 00:00
 Gültigkeitsdauer: 14 Tage
 Berechtigungsprofil: MA
 Alle Berechtigungen: Einbauort Bereich Zeitprofil
 Individuelle Berechtigungen: Einbauort / Bereich Zeitprofil
 Einbauort: Chief Büro
 Bereich: 302arbeiter
 Zeitprofil: ---
 Datum Ausgabe: 7. Jun. 2018 17:05
 Ausgebender Benutzer: admin

Ausgabe:

Eintrag:

Abbildung 201: Identmedium Ausgabeprotokoll

7.12 Xesar-Zutrittskomponente taufen

Die Xesar-Zutrittskomponenten werden im Baustellenmodus ausgeliefert. Zur Funktion in der Xesar-Anlage muss die Xesar-Zutrittskomponente in die Anlage eingebracht (getauft) werden.

Nach der Definition des Einbauortes in der Xesar-Software ist die Xesar-Zutrittskomponente zum Hinzufügen in die Anlage vorbereitet.

ID	Name	Art	Komponententyp	Zustand im Lebenszyklus
BE01	Büro Dr. Hüber	schwere Tür		Zum Hinzufügen vorbereitet

Abbildung 202: Zutrittskomponente zum Hinzufügen vorbereitet

Zum Hinzufügen einer Xesar-Zutrittskomponente wird in der Xesar-Software eine Konfigurationsaufgabe generiert.

Diese wird auf das Xesar-Tablet synchronisiert und vom Xesar-Tablet mittels Anschlusskabel an der Xesar-Zutrittskomponente ausgeführt.

7.13 Inbetriebnahme des Xesar-Online Wandler Netzwerkadapters EXPERT EX9132CST



Überprüfen Sie, dass Sie das passende Modell zur Inbetriebnahmeanleitung in Verwendung haben, bevor Sie den Netzwerkadapter konfigurieren.

Weitere Netzwerkadapter-Inbetriebnahmeanleitungen:



EVVA Homepage Xesar Downloads

Bei Fragen oder für weitere Informationen wenden Sie sich bitte an an das technische Büro von EVVA.

7.13.1 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)



Abbildung 203: Windows-Adaptereinstellung



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.

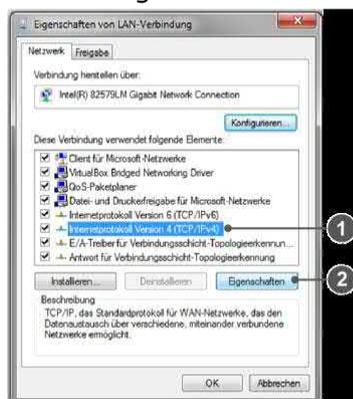


Abbildung 204: Windows - LAN-Verbindung

- » 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: -

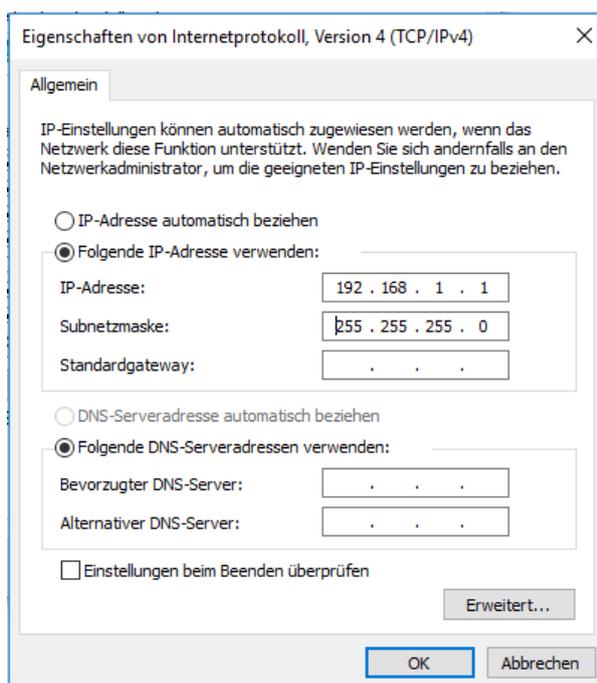


Abbildung 205: Windows – IP-Adresse (PC)



Um einen IP-Adressenkonflikt zu vermeiden, achten Sie darauf, dass Sie **NICHT** die voreingestellte IP-Adresse des Xesar-Netzwerkadapters (**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.

7.13.2 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.

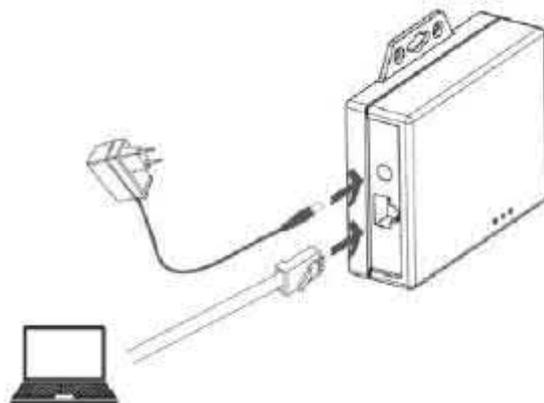


Abbildung 206: Xesar-Netzwerkadapter – Anschlüsse

- » 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.

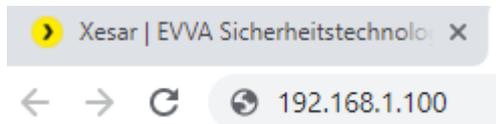


Abbildung 207: Xesar-Netzwerkadapter - IP-Adresse (Updater)



Wenn Sie die Konfigurationsseite nicht öffnen können, kontrollieren Sie die Firewall- Einstellung Ihres PC, die IP-Einstellungen und die korrekte Verkabelung des Xesar-Netzwerkadapters.

Sie gelangen zur System-Seite des Xesar-Netzwerkadapters.

7.13.3 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.



Abbildung 208: Xesar-Netzwerkadapter – Login

7.13.4 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.

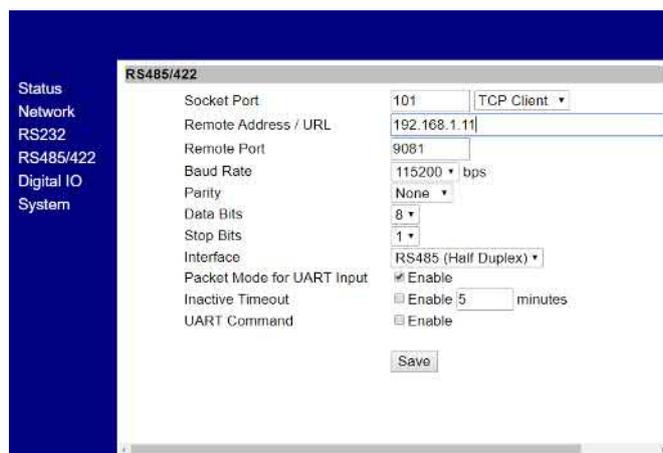


Abbildung 209: Xesar-Netzwerkadapter - RS485/422

7.13.5 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.

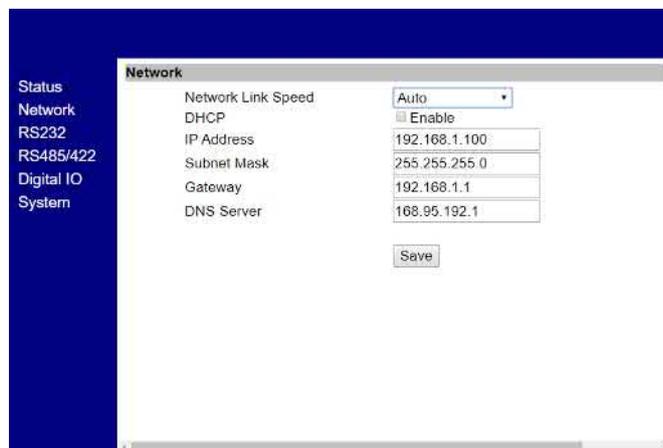


Abbildung 210: Xesar-Netzwerkadapter – Network

- » Klicken Sie nach Abschluss der Parametrierung auf **Save**, um die Konfiguration des Xesar-Netzwerkadapters abzuschließen
- » Zum Übertragen der Daten an den Xesar-Ethernetadapter drücken Sie „Reboot“.

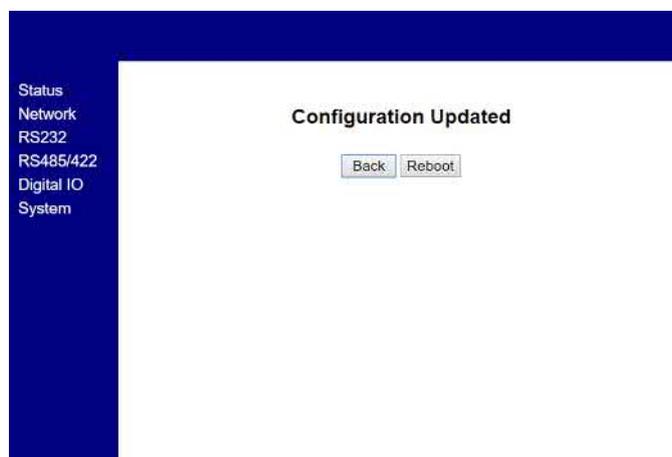


Abbildung 211: Xesar-Netzwerkadapter - Parameter setting

- » Trennen Sie nach dem Rebooten des Netzwerkadapters den Xesar-Netzwerkadapter vom Konfigurations-PC. Schließen sie nun den Xesar-Netzwerkadapter an das Xesar LAN Netzwerk an

Bei den bis zu **typisch150** 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

7.13.6 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 zurücksetzen (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)!

RS485/422	
Socket Port	101 TCP Client ▾
Remote Address / URL	192.168.1.11
Remote Port	9081
Baud Rate	115200 ▾ bps

Abbildung 212: Port

8 Xesar-Systemverwaltung

Alle Installationen, wie Xesa-Software, Xesar-Periphery Manager wurden erfolgreich durchgeführt. Die Xesar-Systemverwaltung gibt einen Überblick über die täglichen Aufgaben der Xesar-Software und deren Verwaltungsoberfläche (Xesar-Dashboard) und Features.

8.1 Starten und Beenden von Xesar

» Klicken Sie auf den von Ihrem Administrator bereitgestellten Link (Server)

oder

» Klicken Sie im Xesar-Installation Manager oder Xesar-Periphery Manager auf das Symbol **Gehe zu** 



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

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

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

Das Symbol des Xesar-Periphery Managers  ist in der Taskleiste.



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

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

8.2 Das Xesar-Dashboard

Das Xesar-Dashboard bietet eine übersichtliche Darstellung der Funktionen von Xesar.

Das Xesar-Dashboard ist der Arbeitsplatz, auf dem Identmedien, Personen, Türen, Bereiche und Berechtigungen verwaltet werden. Zusätzlich werden auf dem Xesar-Dashboard Warnungen, wie unsichere Identmedien und Einbauorte sowie Hinweise, wie Wartungsaufgaben (Batteriestatus und Firmwarestatus) angezeigt.

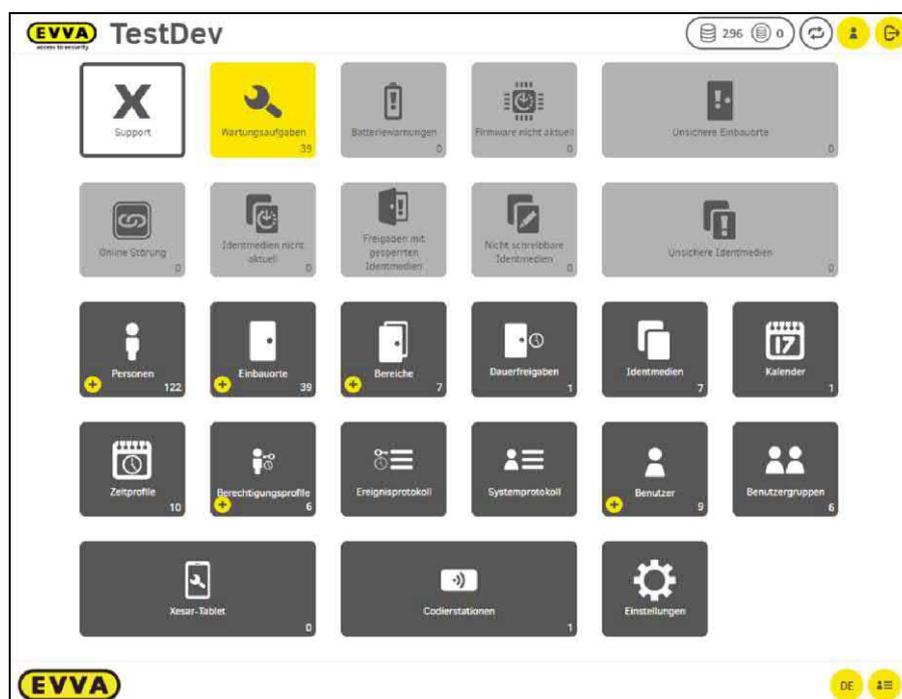


Abbildung 213: Xesar 3-Dashboard

Das Xesar-Dashboard setzt sich aus Kacheln (Felder) zusammen, deren Farbe verschiedene Funktionen signalisieren:

- Dunkelgraue Kacheln dienen zur Verwaltung, wie z.B. Erstellung von Bereichen, Einbauorten oder Berechtigungsprofilen.
- Hellgraue Kacheln bedeuten, dass keine Aktion gesetzt werden muss.
- 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.

8.3 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.

8.3.1 Manuell filtern

- » Klicken Sie auf das Symbol **Filterbereich öffnen** ①
- » Wählen Sie die gewünschten Filterkriterien aus ②
- » Klicken Sie auf Filtern ③

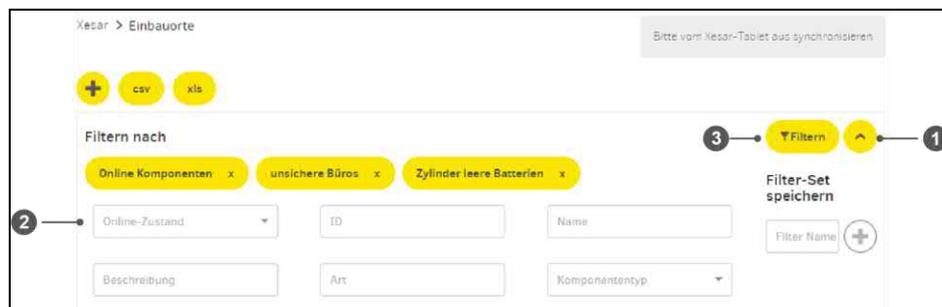


Abbildung 214: manueller Listenfilter

8.3.2 Filter-Presets

- » Klicken Sie auf das Symbol Filterbereich öffnen ①
- » Wählen Sie die gewünschten Filterkriterien aus ②
- » Vergeben Sie einen Namen für Ihr Filter-Preset ③
- » Klicken Sie auf das Symbol **Hinzufügen** ④

Klicken Sie auf das Symbol **x** ⑤ im Button Feld, um das Preset zu löschen.

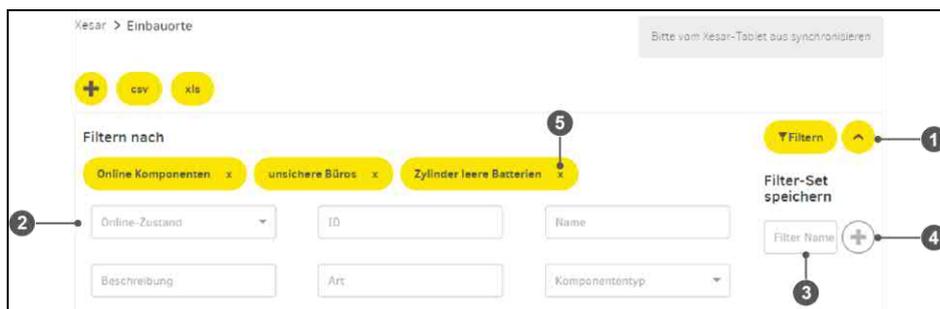


Abbildung 215: Filter-Preset erstellen

Filter-Preset anwenden:

- » Klicken Sie zum Aktivieren auf den Button für das **Filter-Preset** ①|④
Die Filterkriterien ② werden angezeigt
Die Filterergebnisse ③ werden in der Liste angezeigt
- » Klicken Sie nochmals auf den Button für das Filter-Preset ①|④ oder auf den Button **Filtern** ④, um die Funktion Filter zu beenden.

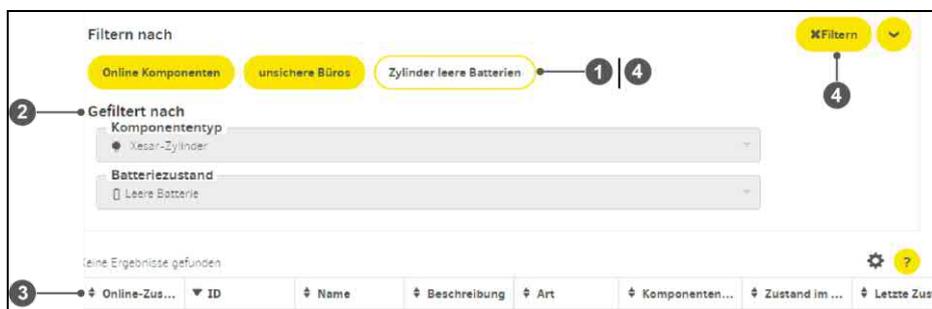


Abbildung 216: Filter-Preset anwenden



Die Anzahl der Filter-Presets je Liste ist nicht beschränkt.

8.3.3 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.



Abbildung 217: Anpassung der Listenansicht

8.4 Mein Profil

Der Menüpunkt **Mein Profil**  befindet sich in der oberen rechten Ecke des Xesar-Dashboards. (Alternativ gelangen Sie über das Feld **Benutzer** und Auswahl des Benutzerkontos zur Seite **Mein Profil**.)

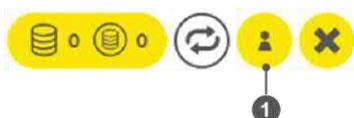


Abbildung 218: Mein Profil

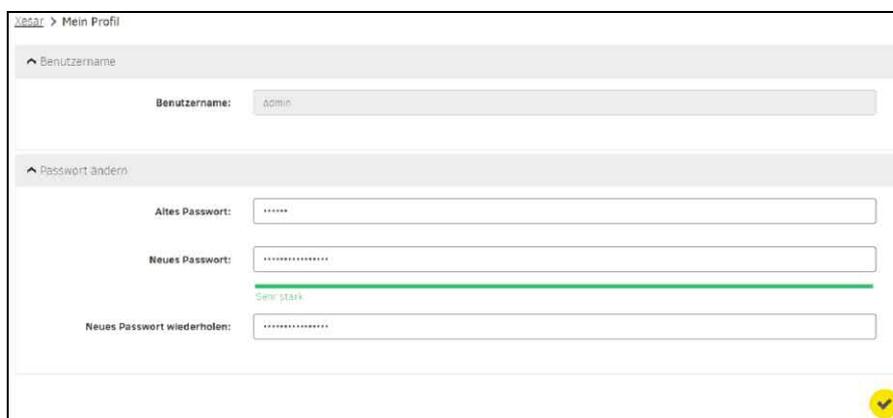


Abbildung 219: Mein Profil

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).



Wenn Sie Ihr Benutzer-Passwort vergessen haben, kann nur der System-administrator (su) ein neues Passwort vergeben.

8.5 KreyCredits (Stück)

Am Xesar-Dashboard wird das aktuelle Guthaben und abzubuchende KeyCredits ¹ angezeigt.

Kostenpflichtige Änderungen betreffen

- Neuausstellung von Identmedien
- Berechtigungsveränderungen

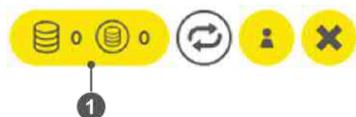


Abbildung 220: KeyCredits Anzeige



Sperren oder der Entzug von Berechtigungen ist kostenlos.



Abbildung 221: KeyCredits – keine Änderungen

Kostenpflichtige Änderungen werden direkt bei der Erstellung oder Änderung von Berechtigungen am Identmedium angezeigt.



Abbildung 222: KeyCredits – kostenpflichtige Änderung

» 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 Xesar-Dashboard. (Beachten Sie die Informationen zum Aufladen der KeyCredits im Kapitel 5.1 Xesar-Installation Manager)

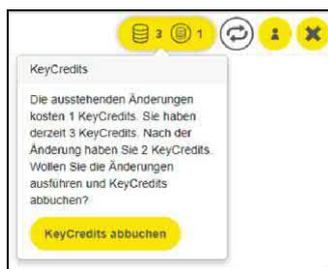


Abbildung 223: KeyCredits – kostenpflichtige Änderung durchführen



Bei Keycredit Xesar-Lifetime sind alle Berechtigungsänderungen und Ausstellungen von Identmedien inkludiert und müssen nicht bestätigt werden.

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden
Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

8.6 Support



Abbildung 224: Kachel Support

Auf der Xesar-Support Seite werden folgende Support-Optionen angeboten:



Abbildung 225: Xesar-Support Seite

8.6.1 Über Xesar

- EVVA Impressum ❶
- Installierte Xesar-Version mit den Versionen des Installation Managers, Xesar-Periphery Managers und Xesar-Tablet App ❷
- Ausgelieferte Firmware-Versionen der Xesar-Zutrittskomponenten ❸
- Link zu den Allgemeinen Lizenzbedingungen von EVVA (mit Download-Möglichkeit) ❹



Abbildung 226: Über Xesar

8.6.2 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.

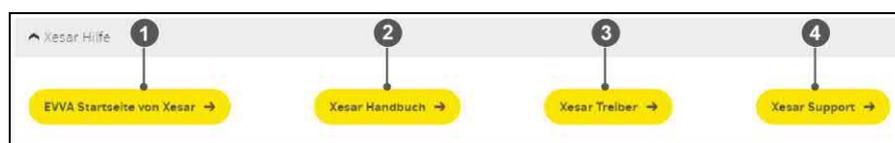


Abbildung 227: Xesar-Hilfe

8.6.3 Aktualisierung

- Download der aktuellen Xesar Tablet APP ❶.
- Download des aktuellen Xesar Periphery Managers ❷



Abbildung 228: Aktualisierung

8.6.4 Supportinformationen herunterladen

Sie können bestimmen, welche Supportinformationen zusammengefasst werden.

- Statistische Informationen einbeziehen (z.B. Anzahl von Einbauorten, Bereichen, Personen, Identmedien, gesperrten Identmedien oder Einbauorte pro Bereich) ❶.
- Alle oder limitierte Anzahl der Ereignisse ❷.
- Download der Supportinformationen ❸.



Abbildung 229: Aktualisierung



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.


SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

9 Wartungs- und Konfigurationsaufgaben



Abbildung 230: Kachel Wartungsaufgaben

Wartungsaufgaben sind alle Konfigurations- und Wartungsaufträge, wie:

- Batteriewarnungen und Zustände
- Xesar-Zutrittskomponenten
 - Konfigurieren
 - Entfernen
 - Hinzufügen
 - Firmware-Update
- Der Name des Xesar-Tablets, welchem die Wartungsaufgabe zugewiesen wurde

Die Kachel **Wartungsaufgaben** ist gelb, wenn eine neue Aufgabe vorhanden ist. Diese wird automatisch vom System erstellt, sobald eine Xesar-Zutrittskomponente gewartet werden muss.



Die Wartungsaufgaben werden mit dem Xesar-Tablet an den Xesar-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 Identmedium 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 f Wartungsaufgaben offen sein.)

Achtung: Dies gilt nicht für Upgrades von Xesar 2.2 auf Xesar 3.x.

9.1 Firmware Update



Abbildung 231: Kachel Firmware nicht aktuell

Die Kachel **Firmware nicht aktuell** ist hellgrau, wenn keine Aufgaben offen sind. Gegebenfalls wird sie gelb und zeigt an, bei welchen Xesar-Zutrittskomponenten die Firmware aktualisiert werden soll. Eine Aktualisierung der Firmware bietet die Vorteile:

- Mögliche Fehler wurden behoben
- Die Batterielebensdauer wurde durch Anpassungen erhöht
- Neue Funktionen sind hinzugefügt worden



Es wird automatisch eine Wartungsaufgabe kreiert, falls eine Xesar-Zutrittskomponente nicht über die aktuelle Firmware verfügt.



Ein Firmware-Update kann auch ohne **Taufe** oder **Hinzufügen einer Xesar-Zutrittskomponente** in eine Anlage erfolgen.


SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

9.2 Batteriewarnung



Abbildung 232: Batteriewarnung

Die Kachel **Batteriewarnungen** wird gelb und zeigt alle Xesar-Zutrittskomponenten an, bei denen die Batterie schwach ist und ersetzt werden soll.



Für alle betroffenen Xesar-Zutrittskomponenten wird eine Wartungsaufgabe erstellt.

9.3 Codierstationen



Abbildung 233: Kachel Codierstationen

In der Kachel **Codierstationen** sind alle aktiven und inaktiven verwendeten Codierstationen aufgeführt.



Sie benötigen eine aktive Codierstation, um Identmedien auszustellen oder updaten zu können.



Installieren und konfigurieren Sie den Xesar-Periphery Manager, um die Xesar-Software und Ihre Anlage mit der Codierstation zu verbinden. (Siehe Kapitel 5.5 Codierstation mit der Xesar-Software verknüpfen.)

9.4 Online-Störung



Abbildung 234: Kachel 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 Identmedien an diesem Xesar-Online Wandleser aktualisiert werden.

Bitte prüfen Sie ob:

- Ihr Xesar-Netzwerkadapter richtig eingestellt ist
- Die Xesar-Steuereinheit richtig mit dem Xesar-Netzwerkadapter verbunden ist

Unsichere Einbauorte



Abbildung 235: Unsichere Einbauorte

Die Kachel **Unsichere Einbauorte** wird gelb, wenn ein Identmedium gesperrt wurde und die Blacklist an den Einbauorten nicht aktuell ist.

Die Blacklist-Aktualisierung kann durch das XVN oder durch eine Synchronisation zwischen Xesar-Software und Xesar-Zutrittskomponente mit dem Xesar-Tablet erfolgen.



Es wird automatisch eine Wartungsaufgabe erzeugt, sobald ein unsicherer Einbauort existiert.

9.5 Identmedien



Abbildung 236: Identmedien

Für Xesar stehen verschiedene Formen von Identmedien zur Verfügung. (siehe Kapitel 2.8 Xesar-Identmedien).

Die Anzahl der angezeigten Identmedien ist unabhängig davon, ob sie z. B. gesperrt oder unbeschrieben sind.

Identmedien – Stapelverarbeitung

In Xesar gibt es mit der Stapelverarbeitung die Funktion, schnell und einfach mehrere Identmedien zur Xesar-Anlage hinzuzufügen. Die Funktion Stapelverarbeitung ist in der Kachel **Identmedien** im Menüpunkt **Hinzufügen – Stapelverarbeitung** ①.

ID	Name B...	Person	Datum Ausgabe	Letzte Synchroni...	Gültig bis (Ident...	Ausgeb...	Zustand	Aktuell	S...	Individuelle Berechtig...
KDM1	Keine Bere...	Huber, Mar...	4. Dez. 2017 18:09	4. Dez. 2017 18:33	23. Dez. 2017 16:30	admin	🔄	🟡	33	Item
KPM2	Chris Stoner	Stoner, Ch...	4. Dez. 2017 18:12	4. Dez. 2017 18:12	18. Dez. 2017 14:19	admin	🔄	🟡	33	Item

Abbildung 237: Liste Identmedien

Um mit der Stapelverarbeitung zu beginnen, geben Sie die aktuelle Laufnummer ID ein, um den Identmedien 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 Identmedium auf die Codierstation.



ID ist z.B. die Personalnummer



Abbildung 238: Stapelverarbeitung aktivieren

Über **Stapelverarbeitung deaktivieren** wird die Stapelverarbeitung gestoppt.



Abbildung 239: Stapelverarbeitung deaktivieren

9.5.2 Identmedium einziehen

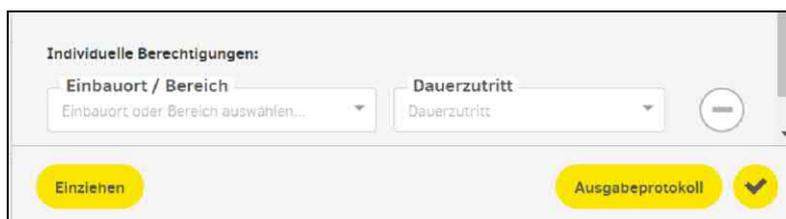


Abbildung 240: Identmedium einziehen

Ein Identmedium 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 Identmedium gelöscht; es kann wieder neu beschrieben werden.

Das Identmedium bleibt in der Liste der Identmedien erhalten.



Das Einziehen eines Identmediums löscht alle Daten, außer dem Schlüssel ihrer Installation im Speicher.

9.5.3 Identmedium Berechtigung entziehen

Für nicht kritische Identmedien (z. B. Identmedien von Personen, die keinen Zugang mehr haben sollen, z. B. Fremdfirmen im Gebäude) gibt es die Funktion **Berechtigung entziehen** ①. Bei Entzug einer Berechtigung eines Identmediums wird kein Blacklisteintrag erstellt und am Xesar-Dashboard wird keine Warnmeldung angezeigt.

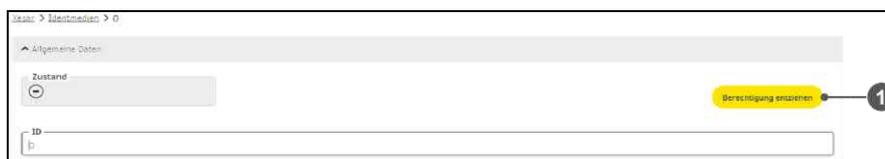


Abbildung 241: Identmedium – Berechtigungen entziehen

- » Klicken Sie am Xesar-Dashboard auf den Menüpunkt Identmedien und wählen Sie das betroffene Identmedium aus.

9.5.4 Identmedium sperren (auf Blacklist setzen)

Ein Identmedium, das Sie sperren ①, wird automatisch auf eine Blacklist gesetzt. Die Blacklist gilt als Sicherheitsrisiko-Liste. Personen mit gesperrten Identmedien haben solange Zutritt, bis jede einzelne betroffene Xesar-Zutrittskomponente aktualisiert wurde. Das kann entweder über Wartungsaufgaben mit dem Xesar-Tablet oder über das XVN erfolgen.



Abbildung 242: Identmedium sperren (auf die Blacklist setzen)



Am schnellsten wird die Anlage via XVN (Xesar-Virtuelles Netzwerk) gesichert.

Im Xesar-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 Identmedien** ändern ihre Farbe auf gelb.

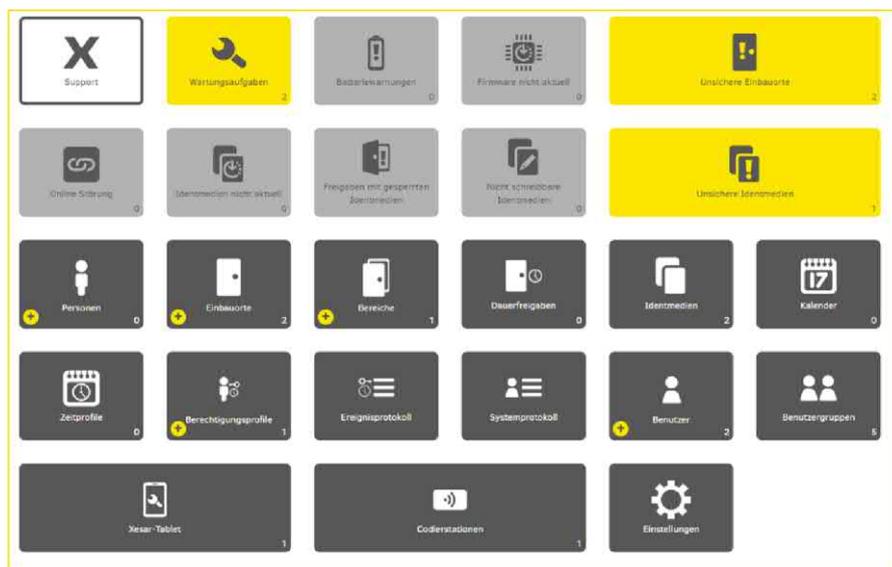


Abbildung 243: Xesar-Dashboard Blacklist

9.5.5 Nicht schreibbare Identmedien

Die Kachel **Nicht schreibbare Identmedien** signalisiert, dass bei bestimmten Identmedien der interne Kartenspeicher (Aktuell: 4k Bytes) voll beschrieben ist. Die Kachel ist gelb – eine Sicherheitsvorkehrung, falls sich nicht schreibbare Identmedien im Umlauf befinden. Rechts wird die Anzahl der nicht schreibbaren Identmedien angezeigt.

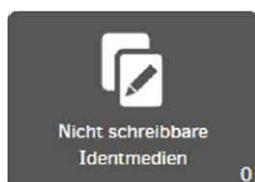


Abbildung 244: Kachel Nicht schreibbare Identmedien



Das Xesar-Segment auf dem Identmedium benötigt etwa 2Kb.



Falls die für Xesar freigegebene Speicherkapazität des Identmediums überschritten wird, färbt sich das Feld gelb. Ein Identmedium kann maximal mit 96 Bereichen bespielt werden. Sollte eine Erweiterung der Berechtigung des Identmedium durchgeführt werden, wird eine Warnung angezeigt.



Zusammenfassen von Bereichen erhöht die Speicherkapazität des Identmediums.

9.5.6 Unsichere Identmedien



Abbildung 245: Kachel Unsichere Identmedien

Unsichere Identmedien entstehen durch das Sperren von Identmedien. In diesem Zustand kann das gesperrte Identmedium trotzdem noch Zutrittskomponenten öffnen. (Siehe 9.5.4 Identmedium sperren (auf die Blacklist setzen))

9.5.7 Identmedien nicht aktuell



Abbildung 246: Kachel Identmedien nicht aktuell

Nach bestimmten Funktionen, z. B. nach einer Berechtigungsänderung müssen Identmedien aktualisiert werden. Das Feld färbt sich gelb und zeigt somit an, dass Identmedien nicht aktuell sind und aktualisiert werden müssen.



Identmedien können über die Codierstation oder durch den Xesar-Online Wandler aktualisiert werden.

9.5.8 Freigaben mit gesperrten Identmedien

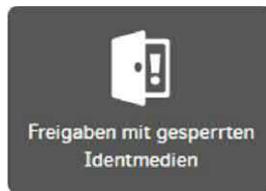


Abbildung 247: Kachel Freigaben mit gesperrten Identmedien

Die Kachel **Freigaben mit gesperrten Identmedien** zeigt an, ob und wo Freigaben mit gesperrten Identmedien erfolgt sind.



Halten Sie die Xesar-Anlage mit Wartungsaufgaben und XVN-Funktionalität aktuell.

9.6 Protokolle

In Xesar werden zwei Arten von Protokollen unterschieden:

- Ereignisprotokoll
- Systemprotokoll

9.6.1 Ereignisprotokoll



Abbildung 248: Kachel 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 Xesar-Zutrittskomponenten) ausgelöst werden.



Die Ereignisprotokollierung ist abhängig von den Einstellungen zum Personenbezug unter Einstellungen sowie von den jeweiligen Protokollierungseinstellungen an den Xesar-Zutrittskomponenten, unter Einbauorte und Protokollierungseinstellungen bei den einzelnen Personen.

Übersicht > Ereignisprotokoll

Kein aktiver Filter

Zeige Einträge 1 - 10 von 44 (44 gesamt)

Datum	Gruppe...	Art des Ereignisses	Ausgabe-Parameter	Person	Name Einbauort	ID Einbauort	ID Identmedium
2017-12-18T14:3...	Konfiguration	Änderung von Datum und Z...		Kein Personenbezug	Hauptingang	AGE1T01	
2017-12-18T14:5...	Konfiguration	Datum und Zeit geändert		Kein Personenbezug	Hauptingang	AGE1T01	
2017-12-18T14:2...	Zutritte	Freigabe mit Identmedium		Kein Personenbezug	Hauptingang	AGE1T01	
2017-12-18T14:2...	Zutritte	Abwekung eines Identmedi...	Invalides Medium	Kein Personenbezug	Hauptingang	AGE1T01	
2017-12-18T14:2...	Zutritte	Abwekung eines Identmedi...	Invalides Medium	Kein Personenbezug	Hauptingang	AGE1T01	
2017-12-18T14:2...	Zutritte	Abwekung eines Identmedi...	Invalides Medium	Kein Personenbezug	Hauptingang	AGE1T01	
2017-12-18T14:2...	Zutritte	Abwekung eines Identmedi...	Invalides Medium	Kein Personenbezug	Hauptingang	AGE1T01	
2017-12-18T14:2...	Zutritte	Freigabe mit Identmedium		Kein Personenbezug	Hauptingang	AGE1T01	
2017-12-18T14:2...	Zutritte	Freigabe mit Identmedium		Kein Personenbezug	Hauptingang	AGE1T01	
2017-12-18T14:2...	Zutritte	Abwekung eines Identmedi...	Medium-ID in Blockiert...	Kein Personenbezug	Hauptingang	AGE1T01	

Abbildung 249: Ereignisprotokoll-Liste

Systemprotokoll



Abbildung 250: 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 Schließsystem ausgelöst werden.

Übersicht > Journal

Kein aktiver Filter

Zeige Einträge 1 - 10 von 119 (119 gesamt)

Kategorie	Beschreibung	Datum	Benutzer	Dent...
	Ein Identmedium wurde aktualisiert.	19. Dez. 2017 11:18	admin	
	Eine Person wurde aktualisiert.	14. Dez. 2017 14:37	admin	
	Ein Identmedium wurde aktualisiert.	14. Dez. 2017 14:37	admin	

Abbildung 251: Systemprotokoll Listenansicht

- » Klicken Sie auf den Button , um den Einbauort direkt aufzurufen und Änderungen vornehmen.

9.7 Xesar-Tablet (Programmiergerät)



Abbildung 252: Kachel Xesar-Tablet (Programmiergerät)

Im Xesar-Tablet befinden sich alle mit der Anlage verknüpften Pro-grammiergeräte.

Klicken Sie auf den Button **Verlust melden** , um das Xesar-Tablet aus der Anlage zu nehmen.



Name	Letzte Synchronisierung	Benutzer	Wartungsaufgaben vorhanden	Verlust melden
Alpha	7. Febr. 2018 09:17	admin	Ja	Verlust melden

Abbildung 253: Verlust melden

9.7.1 Xesar-Tablet App

Am Home-Screen stehen alle offenen Wartungsaufgaben, die Versionsnummer sowie der Button **Synchronisieren**.

Der Home-Screen bietet eine Übersicht aller offenen Wartungsaufgaben, Anzeige der Versionsnummer, sowie den „Synchronisieren“-Button.



Abbildung 254: Xesar-App – Homescreen

Mit einem Klick auf die drei Punkte öffnet sich ein Drop-Down-Menü für:

- Alle Anzeigen
Alle Aufgaben werden angezeigt
- Ausgeführte ausblenden
Die bereits ausgeführten Aufgaben werden ausgeblendet
- Sync-Aufgaben ausblenden
Synchronisationsaufgaben (Logs abholen, Zeit setzen) werden ausgeblendet. Es werden nur die Konfigurationsaufgaben (Konfigurationsänderungen) angezeigt
- Tür erkennen
Erkennt automatisch die angesteckte Tür
- Batteriestatus anzeigen
Der Batteriestatus der Xesar-Zutrittskomponente wird angezeigt
- Firmware aktualisieren
Firmware aktualisieren via Verbindungskabel
- Komponente zurücksetzen
Setzt die Xesar-Zutrittskomponente in ihren Ursprungszustand zurück
- Versionen abfragen
Zeigt die Firmware Version an
- Einstellungen
Festlegung, dass das Ereignisprotokoll der Xesar-Zutrittskomponenten immer abgeholt werden soll
- Ausloggen
Hier loggen Sie den aktiven Benutzer aus

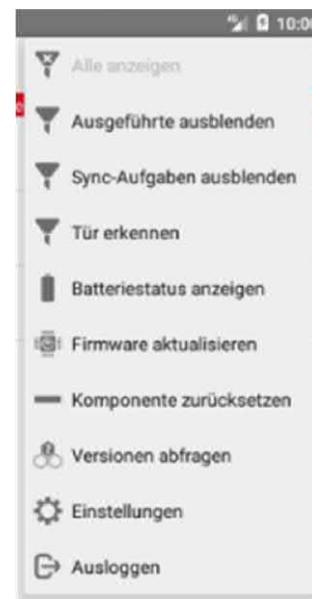


Abbildung 255: Xesar-App - Funktionen

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

9.7.2 Firmware-Update

Ein Firmware-Update an Xesar-Zutrittskomponenten kann sowohl im Baustellenmodus, als auch im eingebauten Zustand durchgeführt werden.

Ist die Xesar-Zutrittskomponente im Baustellenmodus, verbinden Sie für ein Firmware-Update das Xesar-Tablet mit Hilfe des Verbindungskabels mit der Xesar-Zutrittskomponente und wählen Sie Firmware aktualisieren ①.

Ist die Komponente im Anlagenmodus, wird das Firmware-Update über eine Wartungsaufgabe durchgeführt.



Die Firmware-Version der Xesar-Zutrittskomponente kann im Menüpunkt Version abfragen □ ermittelt werden

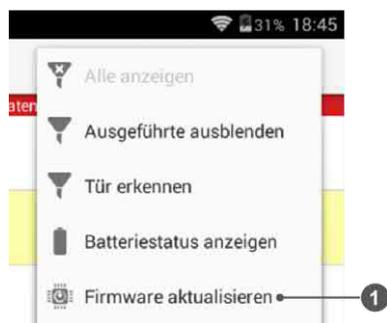


Abbildung 256: Firmware aktualisieren

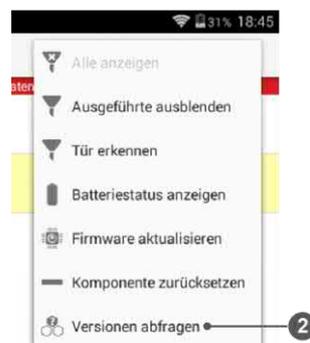


Abbildung 257: Firmware-Version abfragen

9.7.3 Batteriestatus der Xesar-Zutrittskomponente

Verbinden Sie das Xesar-Tablet mit der Xesar-Zutrittskomponente, um manuell den Batteriestatus abzufragen.

Wählen Sie im Dropdown-Menü den Button **Batteriestatus anzeigen** ①.

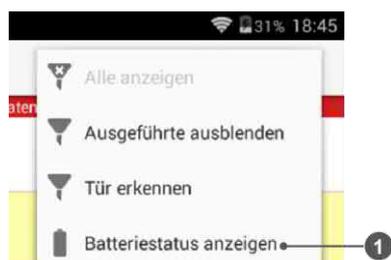


Abbildung 258: Batteriestatus anzeigen

Auf dem Xesar-Tablet wird der Batteriestatus angezeigt.

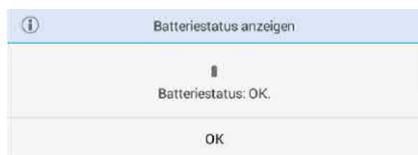


Abbildung 259: Xesar-Tablet - Batteriestatus OK

9.7.4 Xesar-Zutrittskomponente taufen

Um eine Xesar- Zutrittskomponente im Baustellenmodus mit einer Xesar-Anlage zu verbinden, muss diese getauft werden. Zuvor muss ein Einbauort mit Xesar-Zutrittskomponente angelegt werden.

- » Verbinden Sie das Xesar-Tablet mit der Xesar-Zutrittskomponente
- » wählen Sie die Wartungsaufgabe und taufen Sie die Xesar-Zutrittskomponente, indem Sie die Funktion **Ausführen** ❶.

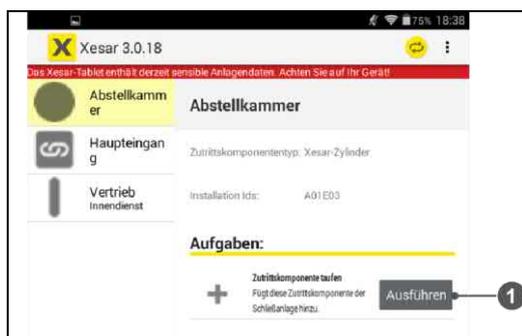


Abbildung 260: Zutrittskomponente taufen

Geben Sie den Tauf-Pin ❷ ein und klicken Sie auf OK. Es startet die Fortschrittsanzeige, mit der Sie die Übertragung verfolgen können.

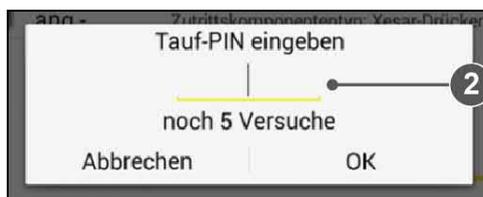


Abbildung 261: Xesar-Zutrittskomponente taufen



Abbildung 262: Xesar-Zutrittskomponente taufen

9.8 Xesar-Virtuelles Netzwerk (XVN)

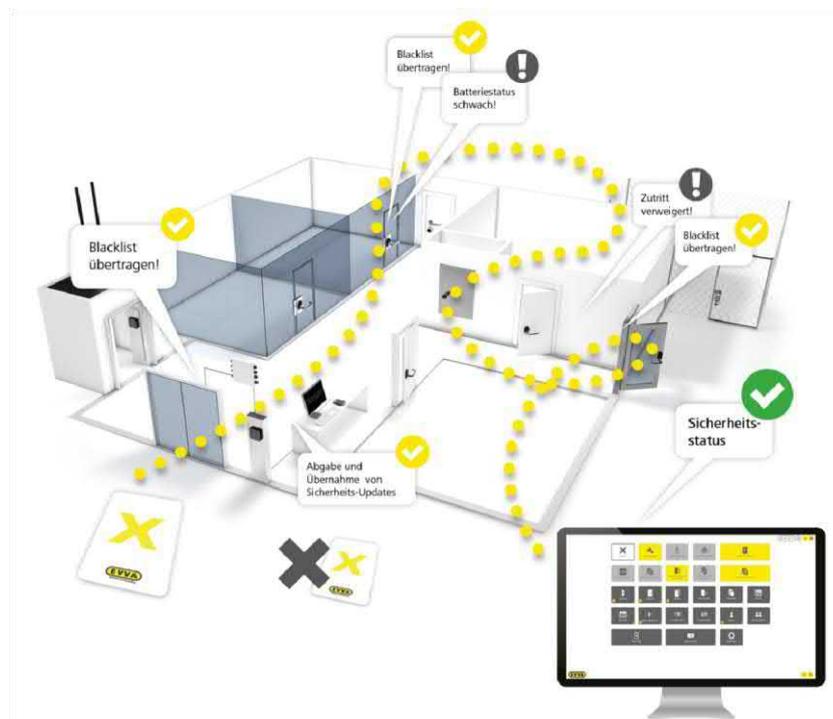


Abbildung 263: Systemüberblick - Virtuelles Netzwerk

An einer zentralen Stelle (Codierstation oder Xesar-Online Wandler) werden die Identmedien mit Update-Informationen (Blacklist) bespielt. Auf dem Weg durch das Gebäude werden diese zu den Türen getragen. Dabei aktualisieren die Identmedien den Status der Türen und sammeln Informationen der Türen (Batteriestatus, Zutrittsereignisse, Löschungen oder Öffnungen von gesperrten Identmedien) ein. An der Codierstation werden diese Informationen abgegeben, ausgewertet und der Sicherheitsstatus in der Software aktualisiert.



Bis zu 150 Xesar-Online Wandler können in eine Anlage eingebunden werden.

9.8.1 Übertragung von Zutrittsereignissen über die Identmedien

Bei jedem zweiten Identifikationsvorgang, z. B. bei der Öffnung einer Xesar-Zutrittskomponente mittels Identmedium, werden die letzten Zutrittsereignisse (z. B. Öffnungen, Abweisungen oder Batterie schwach) der Xesar-Zutrittskomponente auf das Identmedium übertragen.

Wird das Identmedium an die Codierstation oder Xesar-Online Wandlerer gehalten, werden die Ereignisse in die Xesar-Software übertragen und das Medium bereinigt.

Für diesen Vorgang ist ein Login der Xesar-Software nicht notwendig, das gestartete Programm ist ausreichend.

9.8.2 Übertragung von Blacklisteinträgen über die Identmedien

Ein Blacklisteintrag enthält die Information über ein in der Xesar-Software gesperrtes Identmedium. Diese Blacklisteinträge werden via Codierstation oder Xesar-Online Wandlerer auf alle Identmedien geschrieben und so zu allen besuchten Xesar-Zutrittskomponenten getragen.

Auf einem Identmedium sind bis zu 10 Blacklisteinträge möglich. Sobald die Identmedien wieder an der Codierstation oder dem Xesar-Online Wandlerer angehalten werden, erkennt die Xesar-Software, an welche Xesar-Zutrittskomponenten die Blacklist durch das jeweilige Identmedium bereits übertragen wurde und visualisiert den entsprechenden Status am Xesar-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 Identmedium kann ungültig bzw. gelöscht werden, wenn

- das Ablaufdatum überschritten wurde
- die Gültigkeitsdauer überschritten wurde
- das Medium an die Codierstation oder den Xesar-Online Wandlerer gehalten wurde
- das Identmedium versucht, eine Xesar-Zutrittskomponente zu öffnen, bei der die Blacklist aktuell ist.

9.8.3 Übertragung der Information Öffnung durch gesperrtes Medium

So lange ein in der Xesar-Software gesperrtes Identmedium noch gültig ist, kann dieses die jeweiligen Xesar-Zutrittskomponenten auch öffnen. Diese sicherheitskritischen Informationen werden durch andere Identmedien in der Xesar-Anlage gesammelt und via Codierstation oder Xesar-Online Wandlerer an die Xesar-Software übermittelt.

Am Xesar-Dashboard wird das signalisiert. Die Farbe der Kachel **Freigaben mit gesperrten Identmedien** ist gelb, wenn Öffnungen mit bereits gesperrten Identmedien stattgefunden haben.



Abbildung 264: Kachel Xesar-Dashboard - Öffnung durch gesperrtes Medium

9.8.4 Übertragung der Information Identmedium von Türkomponente gelöscht

Bei dem Versuch, mit einem in der Xesar-Software gesperrten Identmedium, eine Xesar-Zutrittskomponente mit aktueller Blacklist zu öffnen, wird das Identmedium von der Xesar-Zutrittskomponente gelöscht.

Anschließend kann dieses Identmedium keine Xesar-Zutrittskomponente ohne aktuelle Blacklist öffnen. Dieses Identmedium hat somit seine Gültigkeit verloren.

Die Informationen von einem gesperrten, gelöschten Identmedium werden von anderen Identmedien via virtuellem Netzwerk zurück zur Xesar-Software übertragen. Dazu müssen die Identmedien an eine Codierstation oder einen Xesar-Online-Wandler gehalten werden.

Die Xesar-Software-Benutzer bekommen so automatisch die Information, dass die Xesar-Anlage wieder sicher ist, obwohl die Blacklist möglicherweise noch nicht bei allen Xesar-Zutrittskomponenten aktualisiert wurde.



Beachten Sie die Hinweise auf eventuelle Wartungsaufgaben im Xesar-Dashboard und halten Sie ihre Xesar-Zutrittskomponenten auf dem neuesten Stand.

FELGNER
SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden
Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

9.8.5 Übertragung des Batteriestatus über die Identmedien

Über die im Umlauf befindlichen Identmedien werden via virtuelles Netzwerk auch Batterie-Informationen 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 Identmedien zu beeinflussen. Die Gültigkeitsdauer wird bei jedem Anhalten eines Identmediums an der Codierstation oder dem Xesar-Online Wandler automatisch um den eingestellten Wert verlängert.

Wird z. B. die Gültigkeitsdauer auf 3 Tage eingestellt, muss jede Person mit Identmedium innerhalb dieser Zeit an der Codierstation oder dem Xesar-Online Wandler 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 Identmedien. 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.

9.9 AdminCard ersetzen

Ist die AdminCard defekt oder verloren gegangen, so kann sie wie folgt ausgetauscht werden:

- » Stecken Sie eine neue AdminCard in die Codierstation
- » Öffnen Sie im Installation Manager den Tab AdminCard und laden Sie die neue AdminCard.
- » Speichern Sie die Einstellung und wechseln Sie zum Tab **Installationen** ①

- » Wählen Sie die gewünschte Anlage **2** aus und klicken Sie auf das Symbol Schlüssel **3**

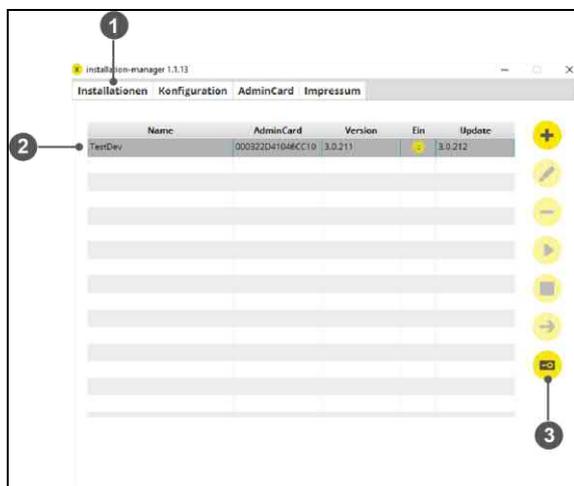


Abbildung 265: AdminCard ersetzen - Xesar-Installation Manager

- » Wählen Sie im Fenster der AdminCard-Operationen die Funktion **Karte tauschen** und
- » geben Sie den Installationsschlüssel, die Kartenummer und die Kartensignatur ein.

Diese Daten finden Sie auf dem Übersichtsblatt Installationsinformationen, das Sie bei der ersten Installation ausgedruckt haben.

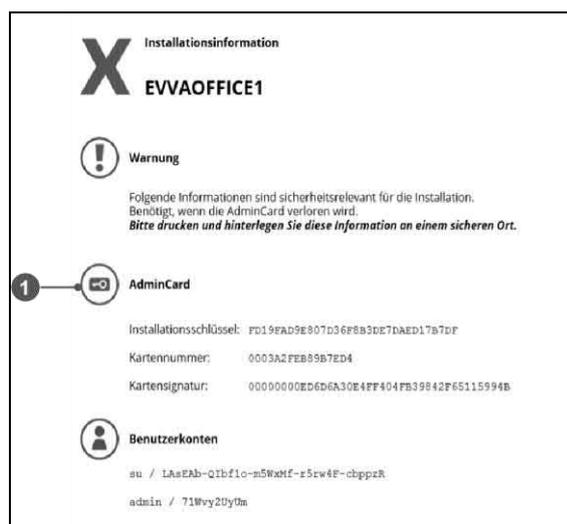


Abbildung 266: AdminCard ersetzen - Anlageninformationen



Abbildung 267: AdminCard ersetzen

Nach Bestätigung wird ein neues Übersichtsblatt Installationinformationen generiert.

- » Drucken Sie das Übersichtsblatt mit den Installationsinformationen aus und bewahren Sie es gut auf.



Erstellen Sie nach dem Tausch der AdminCard unbedingt ein manuelles Backup im Xesar-Installation Manager, damit ein Restore bei Bedarf zur neuen AdminCard passt.

9.10 Komponente hinzufügen rückgängig machen

Falls Sie die falsche Komponente beim Einbauort hinzugefügt haben, können Sie die Komponente wieder entfernen.

- » Klicken Sie auf den Button **EVVA-Komponente hinzufügen rückgängig machen**, am Ende des Eingabefeldes.

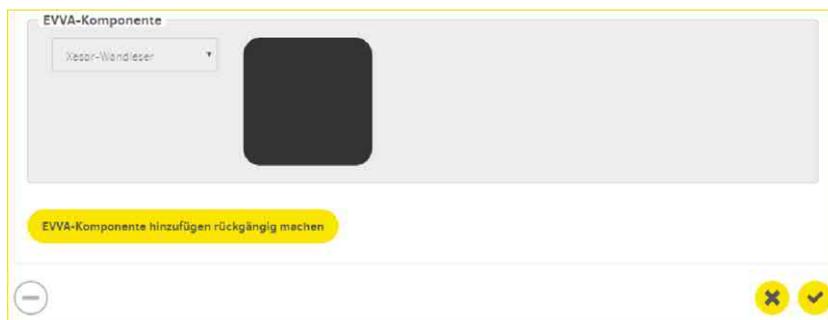


Abbildung 268: Komponente hinzufügen rückgängig machen

Darüber hinaus müssen Sie den Einbauort nicht neu erstellen, sondern können einfach eine neue Xesar-Zutrittskomponente auswählen



Diese Vorgangsweise funktioniert nur vor dem Taufen und falls erforderlich nach dem Rücksetzen in den Baustellenmodus.

9.11 Komponente ausbauen (Rücksetzen in Baustellenmodus)

Wenn eine Xesar-Zutrittskomponente wieder ausgebaut und noch weiterverwendet werden soll, wählen Sie „EVVA-Komponente“ entfernen.

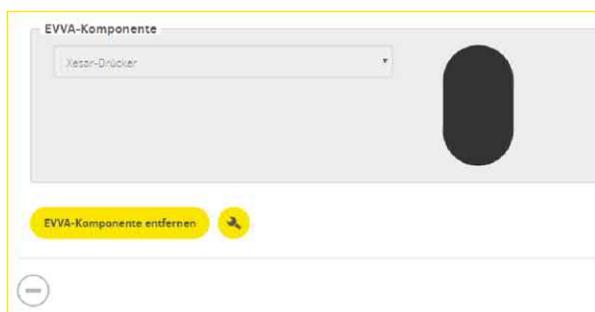


Abbildung 269: Xesar-Zutrittskomponente ausbauen



Wenn Sie die Komponente erneut in der Anlage einbauen wollen, klicken Sie nicht auf **Defekte EVVA-Komponente** entfernen.

Wenn Sie in der Xesar-Software die Xesar-Zutrittskomponente entfernt haben, entsteht automatisch eine Wartungsaufgabe. Es muss die Xesar-Zutrittskomponente mit dem Xesar-Tablet ausgebaut werden. Verbinden Sie die Xesar-Zutrittskomponente mit dem Xesar-Tablet und wählen Sie die Xesar-Zutrittskomponente aus. Im Untermenü klicken Sie auf „Zutrittskomponente entfernen“.

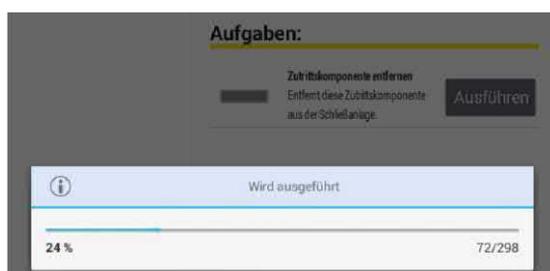


Abbildung 270: Xesar-Tablet - Komponente entfernen

9.12 Komponente erzwungen ausbauen (Komponente defekt)

Wenn eine Xesar-Zutrittskomponente defekt ist, wählen Sie im Menü Einbauorte den entsprechenden Einbauort. Wählen Sie in der Liste die zu entfernende Xesar-Zutrittskomponente und klicken Sie auf **Defekte EVVA-Komponente entfernen**.

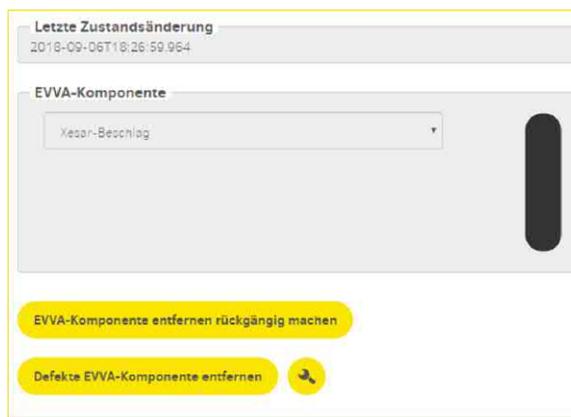


Abbildung 271: Komponente defekt - Ausbau erzwingen

9.13 Xesar-Online Wandlerer



Abbildung 272: Xesar-Online Wandlerer

Der Xesar-Online Wandlerer bietet folgende Funktionen:

- Update von Identmedien
- in Echtzeit
- Zutrittsprotokoll in Echtzeit
- Update der Komponentenberechtigung in Echtzeit
- Xesar-Zutrittskomponente finden: gesuchter Xesar-Wandlerer gibt wiederholend optisches und akustisches Signal bis die Funktion wieder deaktiviert wird
- Office Mode auslösen: Start des Manual-Office Mode (wird protokolliert)
- Office Mode beenden: Beenden des Manual-Office Mode (wird protokolliert).
- Zeit setzen: manuelles Zeitsynchronisieren mit dem Xesar-Online Wandlerer (z.B. nach Stromausfall = Offline) (wird protokolliert).
- Fernöffnung: protokollierte Fernöffnung mit dem Xesar-Online-Wandlerer

- Eine normale Freigabe (Standard-Freigabedauer, wird protokolliert)
- Eine verlängerte Freigabe (Verlängerte Freigabedauer, z.B. für eingeschränkte Personen, wird protokolliert)
- Der Türaustrittstaster wird zum Öffnen von Automatik-Türen oder Vereinzelung verwendet. Jede Betätigung des Türaustrittstasters wird im Ereignisprotokoll protokolliert.
- Die Türzustandsüberwachung ermöglicht die Abfrage des Zustandes (Offen oder Geschlossen) des Türkontaktes. Bei Serienschaltung Türkontakt mit einem Riegelkontakt kann der Türzustand **geschlossen und verriegelt** überwacht werden.

Datum	Gruppe des Ereignisses	Art des Ereignisses	Ausgabe-Parameter	Person	Name Einbauort	ID Einbauort	ID Identmedium
Kein Datum	Konfiguration	Eingabe verändert	Offen	Kein Personenbezug	Online Wandleser	0WLD01	
2018-06-12T12:25:04	Konfiguration	Eingabe verändert	Geschlossen	Kein Personenbezug	Online Wandleser	0WLD01	
2018-06-12T12:25:16	Konfiguration	Eingabe verändert	Offen	Kein Personenbezug	Online Wandleser	0WLD01	
2018-06-12T12:25:12	Konfiguration	Eingabe verändert	Geschlossen	Kein Personenbezug	Online Wandleser	0WLD01	
2018-06-12T12:25:06	Konfiguration	Eingabe verändert	Offen	Kein Personenbezug	Online Wandleser	0WLD01	
2018-06-12T12:25:04	Konfiguration	Eingabe verändert	Geschlossen	Kein Personenbezug	Online Wandleser	0WLD01	
2018-06-12T12:24:58	Konfiguration	Eingabe verändert	Offen	Kein Personenbezug	Online Wandleser	0WLD01	

Abbildung 273: Ereignisprotokoll Türzustandsüberwachung

Die verschiedenen Funktionen werden im Ereignis- und im Systemprotokoll protokolliert.

2018-06-12T16:20:02	Zutritte	Manual Office Mode beendet auf Entfernung
2018-06-12T16:18:54	Zutritte	Manual Office Mode gestartet auf Entfernung
2018-06-12T16:10:18	Zutritte	Verlängerte Freigabe auf Entfernung
2018-06-12T16:01:28	Zutritte	Freigabe auf Entfernung

Abbildung 274: Xesar-Online Wandleser Protokoll



Die Xesar 3.0 Funktionalitäten des Xesar-Online Wandlesers sind in Xesar 2.2 nicht verfügbar (z.B. Online Konfiguration, zeitgesteuerte Online-Konfiguration, Türkontakt).

Der Türtaster kann auch in Xesar 2.2 verwendet werden, das Ereignis wird allerdings in der Xesar 2.2-Software nicht angezeigt

9.14 Mögliche Fehler, die auftreten können

Zertifikationswarnung (dies ist kein Fehler)

Die Zertifikatswarnung wird beim erstmaligen Verbinden und nach der Aktualisierung auf eine neuere Version angezeigt. Das (neu erstellte) Zertifikat muss wieder akzeptiert werden, damit das Arbeiten mit Xesar 3.0 möglich ist.

Docker startet nicht von selbst (Autostart)

Autostart für Docker muss deaktiviert sein. Wurde **Fast Startup** deaktiviert, ist es möglich, dass es durch ein Windows 10-Update (z.B. wie bei Fall Creators Update 2017) wieder aktiviert wird.



Kontrollieren Sie die Einstellung nach jedem Windows-Update, damit Docker weiterhin zuverlässig funktioniert.



Quit and restart Docker

Update auf Xesar 3.0



Nachdem eine Xesar 2.2-Anlage nach Xesar 3.0 importiert wurde, dürfen die Xesar-Zutrittskomponenten nicht mehr mit der Xesar 2.2-Anlage synchronisiert werden. Nach erfolgreichem Import darf nur mehr mit Xesar 3.0 weitergearbeitet werden.

Anzahl der Bereiche in Xesar 3.0 (Vergleich zu Xesar 2.2)

Aus Xesar 2.2 können maximal 95 Bereiche importiert werden. Der 96. Bereich **Installation** wird mit allen Einbauorten in Xesar 3.0 automatisch angelegt.

Import von Xesar 2.2 (Zeitzone)

Eine Xesar 2.2-Anlage kann nur in der gleichen Zeitzone importiert und betrieben werden.

Kalenderimport

Es können keine Kalender (iCal oder CSV) importiert werden, in denen der aktuelle Kalendertag definiert ist. Dies würde zutreffen, wenn Sie z. B. einen Kalender an einem Feiertag anlegen.



Es sollten nur Kalender importiert werden, die zukünftige Einträge ab morgen beinhalten.

Fehler bei der Konfiguration von COM-Ports unter Windows 10

Es gibt einen bekannten Fehler unter Windows 10 in Bezug auf die automatische Konfiguration der COM-Ports



<https://www.tenforums.com/general-support/109079-event-id-10016-distributedcom-windows-securitycenter-wscbrokermanager.html>

Solange dieser Fehler bei Windows nicht behoben wurde, können die Maßnahmen im genannten Artikel angewandt werden, um eine Neukonfiguration der COM-Ports unter Windows 10 durch das Löschen diverser Registry-Einträge zu forcieren. Zudem beschreibt der Windows 10-Fehler das Fehlen von Benutzerberechtigungen dieser COM-Ports, die mit Hilfe dieses Artikels zugewiesen werden können (<http://blog.ronnypot.nl/?p=843>).

Als letzte Maßnahme sollten die Treiber jeglicher COM-Ports de- und wieder installiert werden.

Ablauf von Zertifikaten (Xesar-Tablet, Browser)

Die Zertifikate für die Verbindungen zwischen den Containern bzw. Diensten laufen ein Jahr. Wenn eine Anlage eine überdurchschnittlich lange Zeit (länger als ein Jahr) nicht gestartet wird, laufen diese ab.

In diesem Fall benötigen Sie eine Zertifikatserneuerung, die beim erstmaligen Starten durchgeführt wird. (Die Xesar-Anlage kann in der Xesar-Software nicht ordnungsgemäß verwendet werden und verschiedene Fehlermeldungen werden eingeblendet. Dieser Vorgang regeneriert sich nach wenigen Minuten von selbst.)

Docker kann nicht gestartet werden

Docker kann nur auf Rechnern mit aktivierter Hyper-V Virtualisierung betrieben werden.

Xesar-Lifetime in Xesar 2.2

Xesar-Lifetime darf NICHT in Xesar 2.2 (also vor dem Export/Import nach Xesar 3.0) eingelöst werden! Ansonsten würden in Xesar 2.2 lediglich 17 KCs aufgebucht werden.

Blockieren der Firewall / Verhinderung von Import

Beachten Sie folgende Punkte:

- Die persönliche Firewall muss das Starten grundsätzlich zulassen bzw. darf benötigte Ports nicht blockieren (die virtuelle Maschine 10.0.75.2 muss Zugriff auf den Windows Host 10.0.75.1:445 haben).
- Das Laufwerk C: muss in den Einstellungen von Docker freigegeben sein.
- In den Einstellungen des Docker-Netzwerkadapters den Dienst für "Datei- und Druckerfreigabe für Microsoft-Netzwerke" (File and Print Sharing Service) de- und wieder installieren.
- Gleichzeitig muss der Port 445 für das Docker Netzwerk freigeschaltet werden



<https://docs.docker.com/docker-for-windows/#firewall-rules-for-shared-drives>

Lesefehler von Identmedien

Sollten in einer Xesar-Anlage vermehrt Probleme mit dem Erkennen von Identmedien beim Auflegen auf die Codierstation auftreten, kann es sein, dass der Rechner ein Kommunikationsproblem mit der dazugehörigen Schnittstelle hat. Um dies zu bestätigen muss nach Auftreten des Fehlers in die Windows-Ereignisanzeige (Start -> Ereignisanzeige) navigiert und überprüft werden, ob Fehlermeldungen bezüglich COM-Ports vorhanden sind. Falls ja, kann durch Klicken auf diese die GUID des jeweiligen Ports angezeigt werden. Nach dieser GUID muss dann in der Windows Registry gesucht werden (Start -> regedit eingeben und öffnen -> Suchen nach GUID). Alle Einträge, die diese GUID beinhalten löschen und den Rechner neu starten.

Xesar-Tablet Fehler (ARES FX716M)



Wenn das Xesar-Tablet vom PC abgesteckt wird und sich nicht mehr einschalten lässt, drücken Sie den Reset-Knopf auf der Rückseite des Xesar-Tablets und starten Sie das Xesar-Tablet neu.

Zeitverzögerung beim XVN

Die Aktualisierung der Delta-Blacklist kann bis zu 60 Sekunden dauern.

Xesar-Tablet Fehleranzeige XTDE17

Der Fehler XTDE17 tritt auf, wenn das Zurücksetzen einer Komponente fehlschlägt.

Xesar-Installation Manager erkennt keine Codierstation mehr

Workaround: den Xesar-Installation Manager schließen und erneut starten

Keine Xesar-Dashboard Anzeige im Browser

Falls die Xesar 3.0-Software keine Daten am Xesar-Dashboard anzeigt, liegt das möglicherweise an einer ungewöhnlich hohen CPU Auslastung.

Abhilfe: Die Installation im Installation Manager stoppen und wieder starten.

Bluescreen nach Entfernen eines Mediums von der Codierstation

Es kann auf Windows 7 Rechnern bei Verwendung der HID OmniKey Codierstation 5421 zu Bluescreen Fehlerfällen kommen.

Probleme beim Erkennen von Medien mit Windows 10 Pro x64

Version Build 1709

Tritt dieser Fehler auf, soll ein Update auf Windows 10 Pro x64 Build 1803 durchgeführt werden.

Xesar-Tablet Synchronisation

Wenn eine Konfigurationswartungsaufgabe in die Xesar-Software zurücksynchronisiert wird, dauert es einige Sekunden, bis die Synchronisationswartungsaufgabe dieses Einbauortes auf das Xesar-Tablet kommt.

Xesar-Tablet Synchronisation

Es wird empfohlen, öfter zu synchronisieren. Wenn viele Logs am Xesar-Tablet gespeichert sind, kann die Synchronisierung mehrere Minuten dauern.

Deaktivierung Certificate Propagation Service

Deaktivieren Sie das Certificate Propagation Service auf Windows-Rechnern, die den Periphery-Manager und/oder den Installation-Manager betreiben



[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn579263\(v%3dws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn579263(v%3dws.11))

Kurz Anleitung:

- » **Windows-Taste** und **R** gleichzeitig drücken
- » **services.msc** eintippen und mit **Enter** bestätigen
- » Im neuen Fenster in der Spalte Name den Eintrag **Zertifikatsverteilungsservice** suchen und mit der rechten Maustaste anklicken
- » **Eigenschaften** wählen
- » Im neuen Dialog in der Zeile **Starttyp** den Eintrag **Deaktiviert** auswählen und mit OK bestätigen
- » Alle Fenster schließen und den Rechner neu starten.

Server darf nicht in den Stand-by-Modus schalten

Eine Steuereinheit mit 2 Xesar-Wandlesern

Wenn man eine Steuereinheit mit 2 Xesar-Wandlesern einbaut, sind die beiden Einbauorte miteinander verbunden. Diese Verbindung bleibt auch bestehen, wenn man die Xesar-Zutrittskomponenten entfernt. Direkt nach dem Entfernen der beiden

Xesar-Zutrittskomponenten erreicht man somit wieder den Zustand **zum Einbau vorbereitet**.

Möchte man die beiden Einbauorte löschen, muss man für einen der beiden Einbauorte auf **EVVA-Komponente hinzufügen rückgängig machen** klicken. Dann wird der Button zum Löschen des Einbauorts aktiv und man löscht mittels des einen Einbauorts auch den anderen Einbauort.

Identmedien sperren

Wenn Identmedien gesperrt werden, kann es bis zu 60 Sekunden dauern, bis die aktuelle Delta-Blacklist vollständig auf die Identmedien übertragen wird. Wird vom Zeitpunkt des Sperrens bis 60 Sekunden danach ein Medium aktualisiert (auf Codierstation oder am Xesar-Online Wandler), ist es sehr wahrscheinlich, dass nicht die aktuellste Version auf die Identmedien geschrieben wird.


SICHERHEITSTECHNIK GmbH & Co. KG

■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden

Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service

10 **Abbildungsverzeichnis**

<i>Abbildung 1: Systemarchitektur (Symbolfoto)</i>	13
<i>Abbildung 2: Xesar-Zutrittskomponenten (Symbolfotos)</i>	14
<i>Abbildung 3: Xesar-Beschlag (Symbolfoto)</i>	16
<i>Abbildung 4: Xesar-Drücker (Symbolfoto)</i>	19
<i>Abbildung 5: Xesar-Zylinder (Symbolfoto)</i>	22
<i>Abbildung 6: Xesar-Hangschloss (Symbolfoto)</i>	24
<i>Abbildung 7: Zylinderwerkzeug (Symbolfoto)</i>	26
<i>Abbildung 8: Xesar-Wandleser (Symbolfoto)</i>	27
<i>Abbildung 9: Anschlussprint für Xesar-Wandleser (Symbolfoto)</i>	28
<i>Abbildung 10: Steuereinheit (Symbolfoto)</i>	29
<i>Abbildung 11: Codierstation und Mini-Codierstation (Symbolfotos)</i>	33
<i>Abbildung 12: Xesar-Tablet (Symbolfoto)</i>	34
<i>Abbildung 13: Notstromgerät (Symbolfoto)</i>	37
<i>Abbildung 14: AdminCard (Symbolfoto)</i>	38
<i>Abbildung 15: Identmedien im Überblick</i>	39
<i>Abbildung 16: Construction-Card (Symbolfoto)</i>	40
<i>Abbildung 17: Übersicht Einplatzanlage</i>	41
<i>Abbildung 18: Übersicht Mehrplatzanlage</i>	44
<i>Abbildung 19: Verteilungssicht</i>	53
<i>Abbildung 20: Installation Docker</i>	61
<i>Abbildung 21: Installation Docker - Sicherheitshinweis</i>	62
<i>Abbildung 22: Docker starten</i>	62
<i>Abbildung 23: Docker Startfortschritt</i>	63
<i>Abbildung 24: Docker Statusfensterzeit</i>	63
<i>Abbildung 25: Docker Statusfensterzeit</i>	63
<i>Abbildung 26: Docker Einstellungen-Auswahl (Settings)</i>	64
<i>Abbildung 27: Windows Features</i>	65
<i>Abbildung 28: Windows Features</i>	66
<i>Abbildung 29: Windows Gerätemanager</i>	67
<i>Abbildung 30: Microsoft Treiber aktualisieren</i>	67
<i>Abbildung 31: Treibersuche</i>	68
<i>Abbildung 32: Codierstation - Automatische Treiberinstallation</i>	68
<i>Abbildung 33: Codierstation- Erfolgreiche Treiberinstallation</i>	68
<i>Abbildung 34: Anzeige der Codierstation im Gerätemanager</i>	69
<i>Abbildung 35: Treibersuche (Produkt) bei HID Global</i>	70
<i>Abbildung 36: Treibersuche (Modell) bei HID Global</i>	70
<i>Abbildung 37: Treibersuche (Betriebssystem) bei HID Global</i>	70
<i>Abbildung 38: Treibersuche (Betriebssystem) bei HID Global</i>	71
<i>Abbildung 39: Anwendung Treiberinstallation für Codierstation</i>	72
<i>Abbildung 40: Treiberinstallation für Codierstation</i>	72
<i>Abbildung 41: Treiberinstallation für Codierstation</i>	72
<i>Abbildung 42: Download Xesar-Software</i>	75
<i>Abbildung 43: Xesar-Software Download</i>	76
<i>Abbildung 44: Xesar-Installation Manager zip-Datei</i>	77
<i>Abbildung 45: Xesar-Installation Manager Anwendung</i>	77
<i>Abbildung 46: Xesar-Installation Manager – Warnmeldung</i>	78
<i>Abbildung 47: Xesar-Installation Manager</i>	78

Abbildung 48: Leseinheit im Xesar Installation Manager laden.....	79
Abbildung 49: AdminCard laden	79
Abbildung 50: Xesar-Installation Manager - AdminCard importieren	80
Abbildung 51: Laden.....	81
Abbildung 52: Eine neue Anlage anlegen	82
Abbildung 53: Xesar-Installation Manager - Datenbankimport.....	83
Abbildung 54: Installationsinformationen zur Anlage	84
Abbildung 55: Anlageninformationen exportieren	85
Abbildung 56: Anlagerinformationen	85
Abbildung 57: Software noch nicht gestartet.....	86
Abbildung 58: Anlage wird geladen	86
Abbildung 59: Anlage läuft	86
Abbildung 60: KeyCredits aufladen und aktivieren.....	87
Abbildung 61: KeyCredits-Code eingeben	87
Abbildung 62: Meldungen vom EVVA-Lizenzserver	87
Abbildung 63: KeyCredit Xesar-Lifetime	88
Abbildung 64: Xesar-Installation Manager – Funktionen.....	88
Abbildung 65: Warnhinweise im Browser	89
Abbildung 66: Warnhinweis im Browser.....	89
Abbildung 67: Login-Fenster.....	90
Abbildung 68: Xesar-Dashboard	90
Abbildung 69: AdminCard tauschen	91
Abbildung 70: AdminCard tauschen	91
Abbildung 71: Xesar-Tablet abmelden	93
Abbildung 72: Xesar-Software Update.....	93
Abbildung 73: Xesar-Software Update durchführen	94
Abbildung 74: Xesar-Software Update.....	95
Abbildung 75: Installation sichern.....	95
Abbildung 76: Xesar-Software Update.....	95
Abbildung 77: Meldung Update abgeschlossen.....	96
Abbildung 78: Meldung Update abgeschlossen.....	96
Abbildung 79: Installierte Version nach Update.....	96
Abbildung 80: Xesar-Installation Manager Update.....	97
Abbildung 81: Xesar-Dashboard - Support wählen	98
Abbildung 82: Kachel Support.....	98
Abbildung 83: Xesar-Periphery Manager auswählen.....	99
Abbildung 84: Xesar-Periphery Manager – zip-Datei extrahieren	99
Abbildung 85: Xesar-Periphery Manager zip-Datei extrahieren	100
Abbildung 86: Xesar-Periphery Anwendung.....	100
Abbildung 87: Xesar-Periphery Anwendung - Warnmeldung	101
Abbildung 88: Xesar-Periphery Manager Warnmeldung	101
Abbildung 89: Xesar-Periphery Manager	102
Abbildung 90: Codierstation am Xesar-Dashboard.....	103
Abbildung 91: Kachel Codierstationen	103
Abbildung 92: Codierstation Namen hinzufügen	104
Abbildung 93: Codierstation Status.....	104
Abbildung 94: Codierstation Konfigurationsdatei Download.....	104
Abbildung 95: Xesar-Periphery Manager Konfigurationsdatei hinzufügen	105
Abbildung 96: Xesar-Periphery Manager Konfigurationsdatei auswählen	105
Abbildung 97: Xesar-Anlage im Xesar-Periphery Manager	106
Abbildung 98: Xesar-Periphery Manager Auswahl der Codierstation	106

Abbildung 99: Xesar-Periphery Manager starten	107
Abbildung 100: Xesar-Periphery Manager schließen.....	108
Abbildung 101: Codierstation mit Xesar-Software verbinden.....	109
Abbildung 102: Codierstation-Status Verbunden - Ja	109
Abbildung 103: Windows Command-line CLI	110
Abbildung 104: Xesar-Installation Manager Konfiguration.....	111
Abbildung 105: Xesar-Installation Manager Tablet Web Port.....	111
Abbildung 106: Tablet-App - Login.....	112
Abbildung 107: Xesar-Tablet – Zertifikat 1.....	112
Abbildung 108: Xesar-Tablet – Zertifikat 2.....	113
Abbildung 109: Authentifizierung Xesar-Tablet	113
Abbildung 110: Synchronisierung Xesar-Tablet.....	113
Abbildung 111: Tablet App Home	114
Abbildung 112: Kachel Xesar-Tablet.....	114
Abbildung 113: Xesar-Tablet Einstellungen	115
Abbildung 114: Xesar-Tablet Einstellungen App	116
Abbildung 115: Xesar-Tablet Xesar-App deinstallieren	116
Abbildung 116: Xesar-Tablet App deinstallieren OK	117
Abbildung 117: Xesar-Tablet Datenmanager	117
Abbildung 118: Xesar-Tablet APK löschen	118
Abbildung 119: Desktop – Support auswählen.....	118
Abbildung 120: Kachel Support	118
Abbildung 121: Xesar-Periphery Manager auswählen.....	119
Abbildung 122: Xesar-Tablet APK-Datei.....	119
Abbildung 123: Xesar-Tablet - Xesar 3.0-App.....	120
Abbildung 124: Xesar-Tablet - Xesar 3.0-App installieren.....	120
Abbildung 125: Xesar-Tablet synchronisieren	121
Abbildung 126: Manuelles Backup.....	122
Abbildung 127: Manuelles Backup – Installation sichern.....	123
Abbildung 128: Manuelles Backup – Sicherungsprogramm läuft	123
Abbildung 129: Manuelles Backup -Sicherungsvorgang abgeschlossen	123
Abbildung 130: Manuelles Backup.....	124
Abbildung 131: Automatisches Backup	124
Abbildung 132: Backup Files	125
Abbildung 133: Backup Files	125
Abbildung 134: Anlage entfernen	127
Abbildung 135: Meldung – Installation wird entfernt.....	127
Abbildung 136: AdminCard Nummer Anzeige	128
Abbildung 137: Restore.....	128
Abbildung 138: Restore.....	129
Abbildung 139: Restore.....	130
Abbildung 140: Restore.....	130
Abbildung 141: Restore.....	131
Abbildung 142: Schritt für Schritt-Inbetriebnahme	132
Abbildung 143: Kachel Einstellungen.....	133
Abbildung 144: Sicherheitseinstellungen.....	133
Abbildung 145: Gültigkeits- und Berechtigungsdauer.....	133
Abbildung 146: Systemeinstellungen	135
Abbildung 147: Einstellungen zum Personenbezug	136
Abbildung 148: Standardwert für Einbauorte (Personenbezug).....	136
Abbildung 149: Einstellungen für das Programmiergerät (Xesar-Tablet)	137

Abbildung 150: Kachel Benutzergruppen	137
Abbildung 151: Vordefinierte Benutzergruppen.....	138
Abbildung 152: Benutzergruppe Installationsverwalter	139
Abbildung 153: Benutzergruppen Berechtigungen	140
Abbildung 154: Benutzergruppe Empfang Haupteingang	141
Abbildung 155: Beispiel Zuweisungsmöglichkeit der Berechtigungsprofile einschränken	142
Abbildung 156: Kachel Benutzer.....	142
Abbildung 157: Benutzergruppen	142
Abbildung 158: Adminrechte.....	143
Abbildung 159: Benutzerübersicht	143
Abbildung 160: Neuer Benutzer.....	144
Abbildung 161: Konfiguration herunterladen	145
Abbildung 162: Kachel Kalender.....	145
Abbildung 163: Anzeige der Kalender.....	145
Abbildung 164: Kalender.....	146
Abbildung 165: Kalender importieren.....	146
Abbildung 166: Kachel Zeitprofile	147
Abbildung 167: Manual Office Mode / Shop Mode aktivieren	149
Abbildung 168: Manual Office Mode aktivieren.....	149
Abbildung 169: Ansicht der Zeitprofile.....	150
Abbildung 170: Fehlermeldung Zeitfenster.....	150
Abbildung 171: Manual Office Mode Zeitserienausnahmen:	151
Abbildung 172: Zeitserienausnahme	151
Abbildung 173: Zeitpunktserie	152
Abbildung 174: Ausnahmen zu den Zeitpunktserien	152
Abbildung 175: Zeitprofil hinzufügen.....	153
Abbildung 176: Zeitserienausnahmen	153
Abbildung 177: Kachel Einbauorte	153
Abbildung 178: Anzeige Einbauorte.....	154
Abbildung 179: Einbauort hinzufügen.....	154
Abbildung 180: Einbauort beschreiben	155
Abbildung 181: Freigabedauer	155
Abbildung 182: Zeitprofil (Einbauort)	156
Abbildung 183: Kachel Bereiche	156
Abbildung 184: Ansicht Bereiche	157
Abbildung 185: Anzeige Bereich - Büros	157
Abbildung 186: Auswahl von Einbauorten	158
Abbildung 187: Kachel Berechtigungsprofile.....	158
Abbildung 188: Berechtigungsprofile.....	159
Abbildung 189: Berechtigungsprofil Beispiel - Schichtarbeiter	160
Abbildung 190: Auswahl der Einbauorte	160
Abbildung 191: Zutritt zu ausgewählten Einbauorten.....	160
Abbildung 192: Kachel Personen	161
Abbildung 193: Anzeigen Personenliste	161
Abbildung 194: Person hinzufügen.....	162
Abbildung 195: Kachel Identmedien.....	164
Abbildung 196: Neues Identmedium	164
Abbildung 197: Identmedium zuweisen	165
Abbildung 198: Individuelle Berechtigung	166
Abbildung 199: Identmedium.....	168
Abbildung 200: Identmedium – Individuelle Berechtigung.....	168

Abbildung 201: Identmedium Ausgabeprotokoll	169
Abbildung 202: Zutrittskomponente zum Hinzufügen vorbereitet.....	169
Abbildung 1: Windows-Adaptiereinstellung	170
Abbildung 2: Windows - LAN-Verbindung.....	171
Abbildung 3: Windows – IP-Adresse (PC).....	171
Abbildung 4: Xesar-Netzwerkadapter – Anschlüsse	172
Abbildung 5: Xesar-Netzwerkadapter - IP-Adresse (Updater)	173
Abbildung 6: Xesar-Netzwerkadapter – Login	173
Abbildung 7: Xesar-Netzwerkadapter - RS485/422.....	174
Abbildung 8: Xesar-Netzwerkadapter – Network	174
Abbildung 9: Xesar-Netzwerkadapter - Parameter setting	175
Abbildung 10: Port	176
Abbildung 212: Xesar 3-Dashboard.....	178
Abbildung 213: manueller Listenfilter.....	179
Abbildung 214: Filter-Preset erstellen.....	180
Abbildung 215: Filter-Preset anwenden	180
Abbildung 216: Anpassung der Listenansicht.....	181
Abbildung 217: Mein Profil.....	181
Abbildung 218: Mein Profil.....	181
Abbildung 219: KeyCredits Anzeige.....	182
Abbildung 220: KeyCredits – keine Änderungen.....	182
Abbildung 221: KeyCredits – kostenpflichtige Änderung.....	183
Abbildung 222: KeyCredits – kostenpflichtige Änderung durchführen	183
Abbildung 223: Kachel Support	184
Abbildung 224: Xesar-Support Seite	184
Abbildung 225: Über Xesar.....	184
Abbildung 226: Xesar-Hilfe.....	185
Abbildung 227: Aktualisierung	185
Abbildung 228: Aktualisierung	186
Abbildung 229: Kachel Wartungsaufgaben	187
Abbildung 230: Kachel Firmware nicht aktuell	188
Abbildung 231: Batteriewarnung	189
Abbildung 232: Kachel Codierstationen	189
Abbildung 233: Kachel Online-Störung	190
Abbildung 234: Unsichere Einbauorte.....	190
Abbildung 235: Identmedien.....	191
Abbildung 236: Liste Identmedien	191
Abbildung 237: Stapelverarbeitung aktivieren	192
Abbildung 238: Stapelverarbeitung deaktivieren	192
Abbildung 239: Identmedium einziehen.....	192
Abbildung 240: Identmedium – Berechtigungen entziehen	193
Abbildung 241: Identmedium sperren (auf die Blacklist setzen)	193
Abbildung 242: Xesar-Dashboard Blacklist	194
Abbildung 243: Kachel Nicht schreibbare Identmedien.....	194
Abbildung 244: Kachel Unsichere Identmedien	195
Abbildung 245: Kachel Identmedien nicht aktuell.....	195
Abbildung 246: Kachel Freigaben mit gesperrten Identmedien.....	196
Abbildung 247: Kachel Ereignisprotokoll	196
Abbildung 248: Ereignisprotokoll-Liste	197
Abbildung 249: Systemprotokoll.....	197
Abbildung 250: Systemprotokoll Listenansicht.....	197

Abbildung 251: Kachel Xesar-Tablet (Programmiergerät)	198
Abbildung 252: Verlust melden	198
Abbildung 253: Xesar-App – Homescreen	198
Abbildung 254: Xesar-App - Funktionen	199
Abbildung 255: Firmware aktualisieren.....	200
Abbildung 256: Firmware-Version abfragen.....	200
Abbildung 257: Batteriestatus anzeigen.....	200
Abbildung 258: Xesar-Tablet - Batteriestatus OK	201
Abbildung 259: Zutrittskomponente taufen	201
Abbildung 260: Xesar-Zutrittskomponente taufen	201
Abbildung 261: Xesar-Zutrittskomponente taufen	201
Abbildung 262: Systemüberblick - Virtuelles Netzwerk.....	202
Abbildung 263: Kachel Xesar-Dashboard - Öffnung durch gesperrtes Medium	204
Abbildung 264: AdminCard ersetzen - Xesar-Installation Manager.....	206
Abbildung 265: AdminCard ersetzen - Anlageninformationen	206
Abbildung 266: AdminCard ersetzen	207
Abbildung 267l: Komponente hinzufügen rückgängig machen	207
Abbildung 268: Xesar-Zutrittskomponente ausbauen.....	208
Abbildung 269: Xesar-Tablet - Komponente entfernen.....	208
Abbildung 270: Komponente defekt - Ausbau erzwingen	209
Abbildung 271: Xesar-Online Wandler	209
Abbildung 272: Ereignisprotokoll Türzustandsüberwachung	210
Abbildung 273: Xesar-Online Wandler Protokoll	210



■ Alarmanlagen ■ Schließanlagen ■ Briefkastenanlagen
■ Videoüberwachung ■ Sprechanlagen ■ Zutrittskontrolle

Heiligenbornstraße 17 · 01219 Dresden
Dresdner Straße 177 · 01705 Freital

Telefon: 0351/47 75 20 · E-Mail: info@felgner.de · www.felgner.de

Beratung · Verkauf · Montage · Service