Arckey

Integriertes System für die Verwaltung der Zugänge mit elektrischer Öffnung durch die App

Bedienungsanleitung

Dem Systemadministrator

vorbehaltene

INHALT

WAS IST ARCKEY?

Arckey ist ein integriertes System für die Verwaltung der Zugänge mit elektrischer Öffnung.
Mit der App Arckey, erhältlich für Smartphones und Tablets in Android und iOS, kann man mi kompatiblen Schlössern interagieren und Autorisierungen und Zugangsarten bis zu einer Höchstanzahl von 300 Nutzern, unterteilt in Smartphones, RFID-Karten (z.B. Kreditkarten, U-Bahn-Karte, etc.) PIN-Kombinationen, digitaler Fingerabdruck und Einladung.
Mit der App kann der Systemadministrator auf einfache und innovative Art und Weise im System nicht nur Nutzer hinzufügen, ändern oder löschen, sondern auch die Zugangsregeln konfigurieren, indem er die Nutzung in Standard und „VIP" aufteilt, den Nutzern bestimmte Zeiträume für den Zugang zuteilt, zeitlich begrenzte Zugangsdaten erteilt und vieles mehr.
Der Administrator ist weiterhin auch in der Lage, Nutzer von einem Schloss in andere zu kopieren und jede Aktivität des Zugangsgeräts zu überwachen, indem er die Liste der letzten 1000 aufgetretenen Ereignisse einsieht.

BETRIEBSANFORDERUNGEN

Die App Arckey steht gratis im App Store (iOS) oder in Google Play (Android) zum Download bereit.

Archkey ist kompatibel mit den Geräten

von **iOS** ab iPhone 7 und ab dem Betriebssystem 7.0 und höher
und von **Android** ab der Version 4.3 (Jelly Bean) und höher.

Die App Arckey arbeitet in Kombination mit elektrischen und motorisierten Schlössern, die an Oikos-Türen angebracht sind.
Im Schloss befindet sich ein Elektromotor, der von einem leistungsstarken Mikroprozessor der letzten Generation kontrolliert wird.
Im Falle von mangelnder Versorgung (Akku oder Stromnetz), kann der Türriegel garantiert immer auf traditionelle Weise mit dem mechanischen Schlüssel aufgeschlossen werden.

Vor dem Benutzen von Arckey ist es immer notwendig zu überprüfen, ob das Bluetooth des Geräts aktiviert ist.

ZUGANGSDATEN

Der Zugang von außen kann auf folgende Art und Weise erhalten werden:

Öffnen mit Smartphone und Tablet über die App:

Durch das Klicken auf das **weiße Feld in der App** auf der Startseite eines Smartphones oder Tablets wird das Schloss das Öffnungsbefehl geben (1).

1

Öffnen mit Karte oder Transponder:

Durch das Halten eines Transponderschlüssels (2), einer Oikos Card (3) oder einer Karte mit RFID-Technologie (4) (z.B. Kreditkarte U-Bahn-Karte, etc.) an das externe Lesegerät wird das Schloss das Öffnungsbefehl geben.
Die RFID-Karten müssen MIFARE-kompatibel (13,56 Mhz) sein und müssen generell näher an das Lesegerät gehalten werden (2).

2

3


4

Öffnen mit PIN-Code (nur wenn numerisches Tastenfeld vorhanden):

Durch das Eingeben des numerischen Codes (mindestens 4, höchstens 8 Charakter) und anschließend der Rautetaste # wird das Schloss das Öffnungsbefehl geben (5).


5

Öffnen mit digitalem Fingerabdruck:

Falls an der Tür ein Fingerabdruckleser installiert ist (optional), muss der Finger, dessen Fingerabdruck abgespeichert wurde, an den Leser gehalten werden, damit das Schloss das Öffnungsbefehl gibt (6).


6

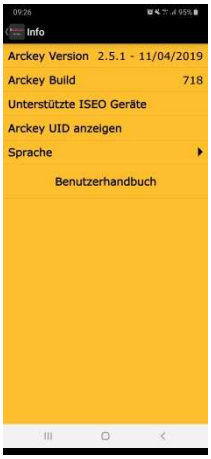
STARTEN VON ARCKEY

Vor dem Start und dem Benutzen von Arckey das Bluetooth auf dem Smartphone aktivieren.

Wenn die App auf dem Display des Smartphones geöffnet ist, werden alle verfügbaren Schlösser in der Reichweite des Bluetoothsignals angezeigt (7).

7

Wenn man auf das Symbol Informationen ⓘ oben rechts klickt, sieht man die Daten über die Appversion und -software der unterstützen Geräte. Es ist auch möglich die Sprache in der App zu ändern und das Benutzerhandbuch in der ausgewählten Sprache anzeigen zu lassen (8).



8

ADMIN CARD

Die **Admin-Cards** erlauben es dem Administrator den Programmiermodus zu öffnen, um das Zugangskontrollsystem von Oikos Arckey zu konfigurieren und verwalten.

ACHTUNG: Das Set mit drei Admin-Cards werden in der Fabrik für interne Qualitätskontrollen versiegelt.
Die Admin Cards in Verwendung ermöglichen es, der einzige Systemadministrator zu werden und die in der vorliegenden Bedienungsanleitung beschriebenen Aktionen durchzuführen. Sorgfältig aufbewahren und Verlieren vermeiden!

Das System (OIKOS Security Code System) sieht drei Sicherheitsstufen für den Zugriff auf die Funktionsparameter des Schlosses vor. Jeder Sicherheitsstufe ist ein Admin Card in unterschiedlicher Farbe zugeordnet:

Grüne Admin Card - Stufe 1
Graue Admin Card - Stufe 2
Rote Admin Card - Stufe 3

Direkt von der ersten Benutzung an kann man auf die Programmierung des Arckey-Systems zugreifen, indem man die grüne Admin Card an das externe Lesegerät hält.
Im Falle des Verlustes der grünen Admin Card (z.B. durch Diebstahl oder Verlieren) kann man jederzeit zu der nächsten Stufe Grau übergehen, indem man einfach die Admin Card der nächsten Stufe Grau an das Lesegerät an der Tür hält. Ein akustisches Signal bestätigt das erfolgreiche Lesen der Card und die grüne Admin Card wird deaktiviert. Auf das zweite akustische Bestätigungssignal nach 10 Sekunden warten.

Im Falle des Verlustes der grauen Admin Card, einfach die rote Admin Card an die Tür halten (ein akustisches Signal bestätigt das erfolgreiche Lesen der Card) und die graue Card wird deaktiviert. Auf das zweite akustische Bestätigungssignal nach 10 Sekunden warten.

Der mögliche Verlust der roten Admin Card verhindert jede Möglichkeit, auf die Programmierung zuzugreifen, um die Funktionalitäten des Arckey-Systems zu verwalten.

Es wird empfohlen in diesem Falle sofort ein neues Admin-Card-Set (Grün-Grau-Rot) anzufordern.

Durch das Halten der grünen Admin Card aus dem neuen Set an die Tür (ein akustisches Signal bestätigt das erfolgreiche Lesen der Card) wird die Funktion des alten Sets deaktiviert und die Originalfunktion wiederhergestellt. Auf das zweite akustische Bestätigungssignal nach 10 Sekunden warten.

Beim Übergehen von einer Admin Card zur nächsten bleiben die System- und Nutzereinstellungen erhalten.

PROGRAMMIERMODUS AKTIVIEREN

Die grüne Admin Card an das externe Lesegerät der Tür halten.

Das Lesegerät gibt ein Leucht- und Tonsignal der Bestätigung, gleichzeitig färbt sich das weiße Feld in der App, das die Tür identifiziert, rot (9).

Auf das Feld klicken.

9

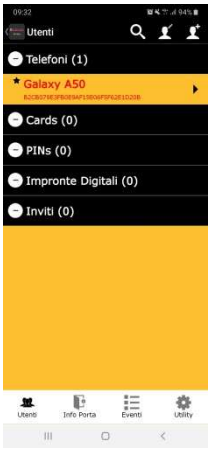
Die App koppelt das Smartphone mit dem Schloss.

SMARTPHONE ALS ZUGANGSGERÄT HINZUFÜGEN

Nach der Kopplung wird gefordert, das Smartphone als Zugangsgerät hinzuzufügen, um das Schloss öffnen zu können (10).
Diese Aktion muss für jedes Smartphone durchgeführt werden, das im Schloss abgespeichert werden soll.

10

Wenn gewünscht, einen Namen für das Smartphone eingeben und auf *Speichern* oben rechts klicken. Nun erscheint das Gerät auf der Übersicht der registrierten Nutzer mit Erlaubnis die Tür zu öffnen (11).
Im Folgenden werden die einzelnen Funktionen im Detail beschrieben:



11

Die Übersicht der Nutzer zeigt eine Liste aller Nutzer, die Zugang zur Tür haben, unterteilt in Zugangsarten: Smartphone und Tablet, Karten (Oikos Card, Karten mit RFID-Technologie, Transponderschlüssel), PIN, digitaler Fingerabdruck und Einladung.

TÜR ÖFFNEN

Programmiermodus schließen, indem man auf das Symbol  oben links klickt.

Auf den weißen Banner klicken, der die Tür identifiziert, um ein Signal an das Schloss zum Öffnen zu schicken. Das Schloss verriegelt die Tür wieder.

SPEICHERN DES NUTZERS

Speichern Oikos Card, Transponderschlüssel, Card mit RFID-Technologie

Programmierung öffnen (siehe S.6).
Sobald man in der Nutzerliste ist, den Schlüssel oder die Card an das externe Lesegerät der Tür halten. Auf das Bestätigungssignal warten. Die Card erscheint nun in der Nutzerliste nach der Speicherbestätigung.

Speichern PIN-Code (nur wenn numerisches Tastenfeld vorhanden).

Programmierung öffnen (siehe S.6).
Sobald man in der Nutzerliste ist, das numerische Code (mindestens 4, höchstens 8 Charakter) und anschließend die Rautetaste # eingeben. Auf das Bestätigungssignal warten. Der PIN-Code erscheint nun in der Nutzerliste nach der Speicherbestätigung.

Manuelles Hinzufügen der Card und der PIN

Es ist möglich Cards sogar ohne ihr physisches Vorliegen hinzuzufügen, indem man ihr Code benutzt. Diese Funktion ist z.B. nützlich, wenn die Karten schon den Nutzern übergeben wurden.
Programmierung öffnen (siehe S.6).

12

13

14

Auf das Symbol *Nutzer hinzufügen* oben rechts klicken und Kartentyp auswählen, die hinzugefügt werden soll (Oikos Card oder generische RFID-Card) (12).
Einen Namen und die Identifikationsnummer auf der Card eingeben. Auf *Speichern* klicken (13).

Wenn man einen PIN eingeben möchte ohne das Tastenfeld zu benutzen, auf *PIN* klicken, einen Namen zuweisen und zwei mal den Code in die Felder *PIN* und *PIN bestätigen* eingeben. Auf *Speichern* klicken (14).

Achtung: Aus Sicherheitsgründen werden die PIN-Codes in der App nie komplett angezeigt.

Speichern von digitalem Fingerabdruck

Programmierung öffnen (siehe S.6).

Auf das Symbol *Nutzer hinzufügen* oben rechts (11) klicken und Digitaler Fingerabdruck auswählen (12).
Der Fingerabdruckleser beginnt zu blinken. Finger wie auf dem Bild auf den Leser platzieren (15).
Die App verlangt, den Fingerabdruck mehrmals abzulesen, um eine Registrierung von hoher Qualität zu erhalten.

15

16

17

Auf *OK* (16) und anschließend auf *Speichern* (17) klicken.
Jetzt wird der Fingerabdruck als gültige Zugangsart erkannt, um die Tür zu öffnen.

Achtung: Zum korrekten Lesen muss der Finger auf den Leser aufgelegt werden und nicht darüber streichen.
Das Lesen des Fingerabdrucks kann sich als schwierig erweisen, wenn z.B. der Finger oder die Oberfläche des Lesegeräts zu feucht ist, die Oberfläche des Lesegeräts nicht sauber genug ist, wenn die Fingerkuppe nicht richtig erkannt werden kann, etc...

Speichern von Einladungen

Einladungen erlauben dem Nutzer (Smartphone oder Tablet) eine Selbstregistrierung in den Speicher des Schlosses als Nutzer mit Zugang durchzuführen, indem er einen Einladungscode benutzt, der vorher vom Administrator im Schloss abgespeichert wurde.

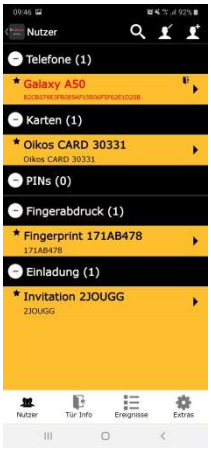
Zum Beispiel kann der Inhaber eines Bed and Breakfast durch diese Funktion dem Gast schon die Erlaubnis erteilen, bevor er überhaupt dort eintrifft.
Um dies durchführen zu können, hat der Administrator im Vorhinein im Speicher des Schlosses einen Einladungscode abgespeichert, der an die Person geschickt werden soll, dem die Erlaubnis erteilt werden soll.

Was muss der Administrator machen, um eine Einladung zu erstellen:

Programmierung der Nutzer öffnen. Auf das Symbol *Nutzer hinzufügen* (11) und dann auf *Einladung* (12) klicken.
Es öffnet sich der Bildschirm für die Nutzerkonfiguration.
Einen Namen eingeben, um diese Einladung zu identifizieren und möglicherweise gewünschte Parameter einzustellen.
Auf **Speichern** klicken, um zu bestätigen.
Es wird gefragt, ob eine Einladungsbenachrichtigung verschickt werden soll (18).
Auf *Ja* klicken, wenn die Benachrichtigung sofort verschickt werden soll oder auf *Nein*, wenn die Benachrichtigung erst später verschickt werden soll.

18

19



20

Es wird automatisch ein Erklärungstext generiert, der Schritt für Schritt erklärt, wie die Einladung benutzt werden soll, um Zugang zur Tür zu erhalten (19).
Außerdem werden Informationen zur Zugangsgültigkeit angezeigt, falls vorhanden (S. 14).
Die Anweisungen können per E-Mail oder Messenger (Skype, WhatsApp, etc.) verschickt werden. Die Einladung erscheint nun auf der Einladungsliste (20).

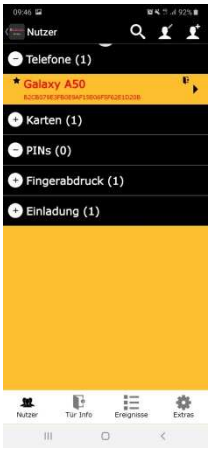
Was muss ein Nutzer machen, wenn er eine Einladung erhält?

Der Nutzer, der eine Einladung erhält, muss zunächst die App auf sein Gerät herunterladen.
Mit aktiviertem Bluetooth und der gestarteten App Oikos Archkey muss sich der Nutzer an die Tür nähern, damit das Schloss erkannt wird. Nachdem Klicken auf das weiße Feld, die die Tür identifiziert, wird aufgefordert den zuvor erhaltenen Einladungscode einzugeben.
Die Tür öffnet sich und das Smartphone erscheint nun in der Liste der registrierten Smartphones.
Wenn die Einladung „akzeptiert" wurde, verschwindet sie von der Einladungsliste.

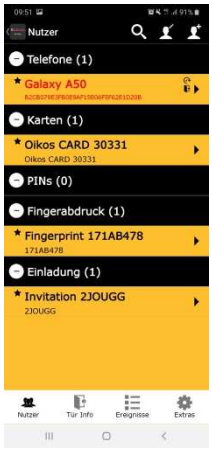
LÖSCHEN UND SPEICHERN VON NUTZERN

Auf das Symbol *Ändern* oben rechts klicken (21).

Den zu löschenden oder speichernden Nutzer auswählen oder auf das Symbol , um alle auszuwählen (22)
(Achtung: Auf diese Weise werden alle Nutzer gelöscht/gespeichert).
Zum Bestätigen des Löschens auf das Symbol *Papierkorb* oder zum Speichern auf das Symbol klicken.



21



22

Die Nutzer werden auf dem Smartphone gespeichert und können falls nötig wiederhergestellt oder auf ein anderes Schloss kopiert werden ohne neu konfiguriert werden zu müssen (siehe S.23).

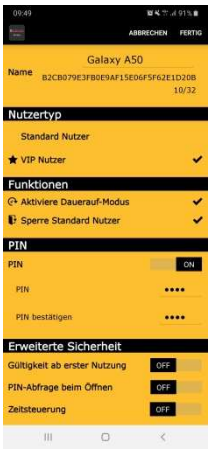
Schnelles Löschen eines Nutzers:

Von der Nutzerliste: Auf Android den zu löschenden Nutzer gedrückt halten. Auf iOS den Nutzer nach rechts „wischen".
Löschen bestätigen.

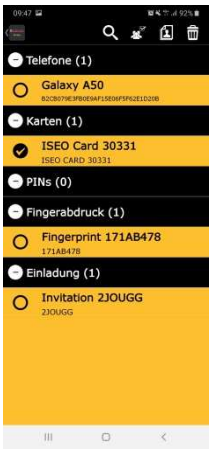
NUTZEREINSTELLUNGEN

Von der Nutzerliste den zu ändernden Nutzer auswählen.

Für alle Arten von Nutzern (Smartphone, Card, PIN, Ablesen des Fingerabdrucks, Einladung) können die gleichen Funktionen und Einstellungen genutzt werden, außer den Folgenden:



23



24

Nutzername: Auf das Feld *Name* klicken, um dem Nutzer auf dem Smartphone oder Tablet einen identifizierenden Namen zu vergeben (maximal 32 Charaktere) (23).

Nutzerart: Auswählen, ob der Nutzer ein Standard- oder VIP-Nutzer ist (23).

VIP-Nutzer: Kann die Tür jederzeit ohne Einschränkungen öffnen. Ihm kann die Befugnis erteilt werden, Standardnutzer zu blockieren. Außerdem kann er den Büromodus aktivieren (siehe S.15).

Standardnutzer: Ihm kann von VIP-Nutzern der Zugriff verwehrt werden. Er kann den Büromodus aktivieren.

Das Symbol ★ in der Nutzerliste zeigt die VIP-Nutzer an (24).

Funktionen: Erlaubt es dem Nutzer den Büromodus zu aktivieren (siehe S. 16) und den Standardnutzern den Zugriff zu verwehren (siehe S. 15) (23). Nur VIP-Nutzer können Standardnutzern den Zugriff verwehren. Den Büromodus kann man durch das Symbol aktivieren und den Standardnutzern kann man den Zugriff durch das Symbol verwehren (24).

PIN-Nutzer (nur für Smartphone-Nutzer): Der Zugang über Smartphone ist durch die Aufforderung einer PIN-Eingabe mittels Smartphone während des Öffnens sicherer, wenn dies vorher bei den Zugangsbeschränkungen festgelegt wurde (25).

25

Das Vorliegen eines PIN-Nutzers wird mit dem Symbol  (24) deutlich gemacht.

Zugangsbeschränkungen: Die Einstellung erlaubt es den Zugang für die Nutzer zu beschränken. Jedem Nutzer können Beschränkungen zugeteilt werden, z.B. eine auf eine bestimmte Anzahl von Tagen festgelegte Zugangszulassung ab dem ersten Tag des Zugangs oder einen voreingestellten Zeitrahmen (Beispiel: Das Servicepersonal kann die Tür nur an einem bestimmten Wochentag um eine bestimmte Uhrzeit öffnen). Für jeden Nutzer können zwei Zeitrahmen erstellt werden.

Falls vorhanden, wird die Zugangsbeschränkung durch das Symbol  angezeigt (24).

Masterphone-Modus (nur für Smartphone-Nutzer): Der Masterphone-Modus erlaubt es dem Smartphone-Nutzer die Programmierung ohne das Vorzeigen der Admin Card zu öffnen, die durch das Smartphone ersetzt wird. Somit kann der Nutzer zum Systemadministrator werden.

Falls eingestellt, kann das Nutzen des Masterphone-Modus durch die Aktivierung eines PIN-Nutzers sicherer gemacht werden.

Die Aktivierung der Masterphone-Funktion erfolgt durch das Symbol Login  oder durch das Symbol Login + PIN  , falls die PIN auch beim Login aktiviert ist (24).

STANDARDNUTZER BLOCKIEREN

Diese Funktion, wenn aktiviert, verwehrt allen Standardnutzern den Zugriff.
Wenn die Einstellung Standardnutzer blockieren aktiviert ist, können nur VIP-Nutzer die Tür öffnen.

Klicken und das Feld, das die Tür identifiziert, bei der die Funktion *Standardnutzer blockieren* aktiviert werden soll, gedrückt halten. Es erscheint nun das Menü zum Aktivieren/Deaktivieren der Funktion (26).

26

Auf dem weißen Feld erscheint ein Symbol ★, das die erfolgte Aktivierung der Funktion anzeigt (27).

27

28

Die Aktion entgegengesetzt ausführen, um die Funktion zu deaktivieren (28).

BÜROMODUS

Die zugelassenen Smartphone-Nutzer (siehe S.13) können auf der Startseite der App den Büromodus aktivieren. In diesem Modus funktioniert das Schloss nur mit Riegel und die Schlüsselbärte werden eingezogen.
In diesem Modus ist die Tür nur angelehnt, aber nicht sicher verschlossen.

Klicken und das Feld, das die Tür, bei der die Funktion *Büromodus* aktiviert werden soll, identifiziert, gedrückt halten. Es erscheint nun das Menü zum Aktivieren/Deaktivieren der Funktion (29).

29

Auf dem weißen Feld erscheint ein Symbol ★, das die erfolgte Aktivierung der Funktion anzeigt (30).

30

31

Die Aktion entgegengesetzt ausführen, um die Funktion zu deaktivieren (31).

Siehe auch S.21 für eine vorprogrammierte Verwaltung des Büromodus.

MASTERPHONE-MODUS

Diese Funktion erlaubt es direkt über das Smartphone auf die Programmierung zuzugreifen, ohne die Admin Card zu gebrauchen. DerNutzer wird zum Systemadministrator.

Klicken und das Feld, das die Tür identifiziert, bei der durch Login auf die Programmierung zugegriffen werden soll, gedrückt halten. Nun erscheint das Menü. (32).
Einloggen durch Klicken auf *Login*.

32

Die Sicherheit kann durch das Hinzufügen eines PIN-Nutzers zur Loginfunktion erhöht werden (siehe S.14).
In diesem Fall wird die PIN abgefragt, um den Zugang zu autorisieren.

ZUGANGSBESCHRÄNKUNGEN

Für jeden Nutzer können befristete Beschränkungen eingestellt werden, entweder als Dauer oder Zeitrahmen.

Gültigkeit ab dem ersten Zugriff: Diese Kontrolle ermöglicht es dem Nutzer eine Gültigkeit „auf Zeit" zuzuweisen.

Es kann z.B. nötig sein, einem Techniker einen befristeten Zugang von zwei Tagen für Wartungsarbeiten zu erteilen. Nach Ablauf des zweiten Tages wird der Zugriff verweigert.
Die Funktion *Gültigkeit ab dem ersten Zugriff* (33) aktivieren und eine Dauer ab dem ersten Öffnen der Tür zuteilen, die in Tagen/Stunden/Minuten angegeben werden kann (34).
Auf *Speichern* oben rechts klicken.

33

34

Zeitüberwachung aktivieren: Ermöglicht es, eine befristete Gültigkeitsdauer für einen Nutzer zu bestimmen (Von einem Datum bis zu einem anderen Datum).

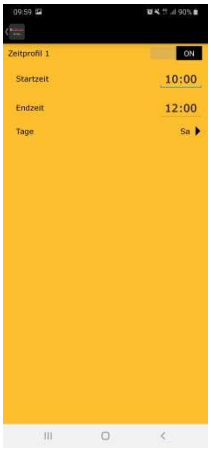
Die Funktion *Zeitüberwachung aktivieren* (35) aktivieren und ein Datum und eine Zeit des Beginns und des Endes angeben (das Ende der Zeit wird automatisch berechnet, wenn eine Anzahl von Tagen angegeben wird). Die Standardeinstellung ist eine Dauer von 20 Jahren (7305 Tage).

In dieser erklärenden Konfiguration wird dieser Nutzer ab dem 22.05.2019 Mitternacht einen unbefristeten Zugriff auf die Tür für 20 Jahre haben.

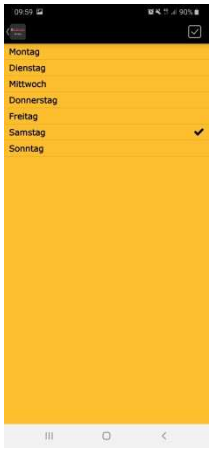
35

Zeitrahmen: Erlauben eine präzisere Kontrolle der Beschränkungen innerhalb der Gültigkeitsdauer. Es ist möglich, die Wochentage und den Zeitrahmen anzugeben, für die die Beschränkungen gelten.

Zum Beispiel: Das Putzpersonal hat eine Zulassung für 20 Jahre, aber nur samstags von 10-12 Uhr (36-37).



36



37

Es können zwei verschiedene Zeitrahmen für eine flexiblere Programmierung der Zugangsbeschränkungen verwaltet werden.

Nach der Konfiguration der Gültigkeitsdauer und eventueller Zeitrahmen oben links auf *Speichern* klicken.

INFO TÜR

Die Übersicht *Info Tür* zeigt die Lister aller entsprechenden Informationen zur zugehörigen Tür:

38

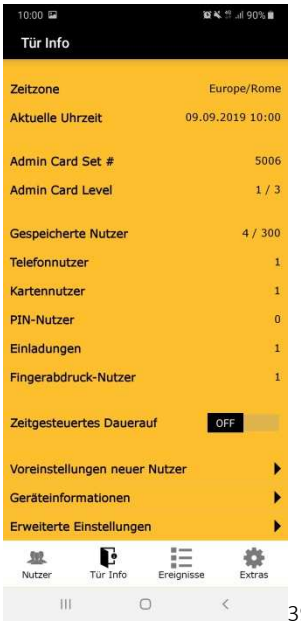
Türname: Kann durch Ersetzen der „Standardtürnummer" personalisiert werden.
Der neu vergebene Name erscheint auf der Startseite der App (38).

Batteriestatus: Zeigt den Akkustand im Inneren des Schlosses an: OK, Low, Very Low, End (38).

Admin Card SET#: Zeigt den Nummerncode an (auf der Rückseite jeder Card angegeben), der das benutzte Cardset identifiziert (38).

Admin-Card-Stufe: Identifiziert die Sicherheitsstufe der aktiven Card (38).

Gespeicherte Nutzer: Gesamtanzahl der registrierten Nutzer unterteilt in Kategorien (maximal 300) (38).



39

Programmierter Büromodus: Erlaubt es den Büromodus im Zeitrahmen zu aktivieren und die Programme 1 und 2 einzustellen (siehe S.21) (39).

Vorbestimmte Nutzereinstellungen: Erlaubt es zu definieren, welche Funktionen den neu erstellten Nutzern standardmäßig zugeordnet werden sollen (ob VIP- oder Standardnutzer, wenn Beschränkungen zu vergeben sind, etc...) (39) (siehe S.13).

Versionen: Die Versionen der Schlosskomponenten werden angezeigt (nützlich falls Hilfe benötigt wird) (39).

Erweiterte Funktionen: Parameter, die **nur** nach Aufforderung des Technischen Supports benutzt werden sollen.

Die Verwendung durch nicht fachmännisches Personal wird abgeraten. Die Änderung der enthaltenen Parameter in den erweiterten Funktionen können die Funktion des Schlosses verändern oder beeinträchtigen.

PROGRAMMIERTER BÜROMODUS

Diese Funktion erlaubt es zwei Programme einzustellen, um automatisch den Büromodus zu aktivieren/deaktivieren. Dies bedeutet, dass das Schloss automatisch in den Büromodus übergeht, indem es bis zu zwei voreingestellten Programmen folgt.

Programmierung und *Türinforrmationen* öffnen (siehe S.6).
Programm 1 aktivieren, um die Konfiguration zu starten. (Für Programm 2 gelten die gleichen Regeln).

Je nach Notwendigkeit können drei verschiedene Nutzungsmodi des Büromodus eingestellt werden:

40

41

42

Büromodus mit automatischer Wiederverschließung:

In diesem Modus erfolgt die Aktivierung manuell durch einen zugelassenen Nutzer (siehe S.12). aber die automatische Wiederverschließung kann auf eine bestimmte Uhrzeit eingestellt werden.
Die Uhrzeit für die automatische Wiederverschließung und die Tage, an dem diese gültig sein sollen, wählen (Der Standard sind Wochentage oder alle Tage außer Samstag und Sonntag).
Auf *Speichern* klicken, um zu bestätigen (40).

Büromodus mit automatischer Aktivierung und Wiederverschließung:

In diesem Modus erfolgen sowohl die Aktivierung, als auch die Wiederverschließung automatisch. Die Uhrzeit für die automatische Aktivierung und der Wiederverschließung und die Tage, an dem diese gültig sein sollen, wählen. Der Standard sind Wochentage oder alle Tage außer Samstag und Sonntag (41).

Büromodus mit automatischer Aktivierung ab dem ersten Zugriff und automatische Wiederverschließung (C):

Der einzige Unterschied im Gegensatz zu den vorherigen Punkten besteht darin, dass die tatsächliche Aktivierung des Büromodus ab dem Zugang durch den ersten zugelassenen Nutzer geschieht. Diese Lösung ist sehr nützlich für die Sicherheit, da vermieden werden kann, dass das Schloss automatisch in den Büromodus wechselt, wenn kein Nutzer im Gebäude oder Raum ist (z.B. könnte der Weihnachtstag auf einen Tag fallen, für den der automatische Büromodus eingestellt ist, aber in diesem Fall dürfte es nicht aktiviert werden) (42).

EREIGNISSE

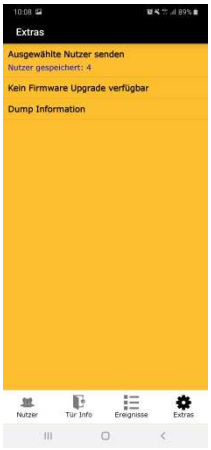
Die Übersicht der Ereignisse zeigt eine Auswahl der letzten 1000 Ereignisse der entsprechenden Tür (43).
Als Ereignis betrachtet man alle mechanischen, elektrischen oder elektronischen Aktionen, die im Schloss erfolgen.

43

Es ist möglich, eine schnelle Suche durchzuführen, indem man den gewünschten Wert in das entsprechende Feld *Suchen* eingibt, nachdem man auf das Lupensymbol 🔍 geklickt hat, um die Ereignisse zu filtern (z.B. alle Ereignisse, die einer bestimmten ID-Card zugehörig sind).
Die Liste kann per E-Mail verschickt werden, indem man auf das Symbol ✉ oben rechts klickt.

UTILITY

In der Übersicht Utility kann man auf die Wartungsfunktionen zugreifen:



44

Gewählte Nutzer verschicken: Die in den Speicher des Smartphones kopierten Nutzer können auf ein anderes Gerät übertragen werden (siehe S.12).
Die Programmierung des Schlosses öffnen, in dessen Speicher die Nutzer kopiert werden sollen (siehe S.7).
Utility öffnen und auf das Feld *Gewählte Nutzer verschicken* klicken (44).
Auf OK klicken, um zu bestätigen (45).

45

Softwareupdate: Updates für die App kontrollieren und herunterladen.
Bei Vorliegen eines verfügbaren Updates genügt es auf das Feld zu klicken, um das Update der Schlosssoftware durchzuführen (42).
Das Smartphone an die Tür halten, bis das Update abgeschlossen ist.

Es wird empfohlen, stets alle Updates herunterzuladen, die von Oikos veröffentlicht werden, um das System auf dem höchsten Sicherheits- und Leistungsstandard halten zu können.

Speicherauszugsinformationen: Erlaubt es per E-Mail alle Diagnosedaten des Schlosses weiterzuleiten. NUR dann zu verwenden, wenn man ausdrücklich vom Service Center von Oikos dazu aufgefordert wird (44).