

Solothurn 10.01.2024

eAccess Mobile Webclient

eAccess Bedienungsanleitung

Index V1.1

Doc-Nr. MA_10165

Glutz AG, Solothurn

Inhaltsverzeichnis

1.	Einleitung	3
2.	Zu diesem Dokument	3
2.1	Abkürzungen & Begriffsdefinition	Fehler! Textmarke nicht definiert.
2.2	Gültigkeit	3
2.3	Kompatibilität und Voraussetzung	3
3.	Einrichtung Webclient	4
3.1	Aktionsprofil	4
3.2	Zugriffsrechte	5
3.3	Standort Einstellungen	6
3.4	System-Informationen für Glutz App vorbereiten	9
3.5	On-Boarding	11
4.	Bekannte Fehler	16
4.1	On-Boarding	16

1. Einleitung

Machen Sie ihr Smartphone zum Schlüssel mit der eAccess Mobile App. Dank der neuen smarten App von Glutz können Türen einfach und sicher mit nur einem Klick geöffnet werden. Die App öffnet Türen, Schranken und Räume ohne Schlüssel oder Badge, sogar von weit weg.

Mit eAccess Mobile erweitern Sie Ihr Zutrittssystem mit vielen neuen Features – die Einsatzmöglichkeiten sind nahezu grenzenlos.

2. Zu diesem Dokument

Dieses Kapitel enthält Informationen für den fachgerechten Umgang mit diesem Dokument.

2.1 Gültigkeit

Dieses Dokument beschreibt das Produkt:

Produktbezeichnung: Glutz eAccess Mobile

Gerätegeneration: Für alle mechatronischen Geräte von Glutz

2.2 Kompatibilität und Voraussetzung

eAccess Mobile ist mit allen bisher verkauften Geräten kompatibel.

Die gewünschten Geräte der eAccess Anlage müssen über das Glutz Netzwerk (NET-Repeater) erreichbar und über ein NET-Gateway mit dem Internet verbunden sein. Weiter muss auch das verwendete Smartphone eine aktive Internetverbindung haben.

Um eAccess Mobile nutzen zu können, wird mindestens die eAccess Software 1.14.0 benötigt.

3. Einrichtung Webclient

Dieser Abschnitt erläutert die neuen Funktionen für Smart Access

3.1 Aktionsprofil

Ab der Version 1.14.0 gibt es einen neuen Identifikations-Typ 'Smart Access (eAccess Mobile)'. Unter *Einstellungen* → *Aktionsprofile* kann das Profil spezifiziert werden.

The screenshot shows a web-based configuration interface for an action profile. It contains the following elements:

- Name:** A text input field containing the value 'Admin'.
- Typ:** A dropdown menu with 'Smart Access (eAccess Mobile)' selected.
- Default Actions:** A horizontal list with one item, 'Kurz öffnen', which has a small 'x' icon to its left and a dropdown arrow to its right.
- Special Actions:** A horizontal list with two items, 'Permanent öffnen' and 'Schliessen', each with a small 'x' icon to its left and a dropdown arrow to the right of the second item.
- Löschen:** A red button with the text 'Löschen' located at the bottom left of the form.

Abbildung 1: Aktionsprofil für eAccess Mobile einrichten

Abbildung 1 zeigt ein Beispiel für ein Smart Access Aktionsprofil, bei welchem ein 'Kurz Öffnen' als Default Action definiert ist. Diese Aktion kann auf der eAccess Mobile App durch ein kurzes Drücken und Halten ausgelöst werden. Die Special Actions können auf der App über das Drop-Down-Menu ausgelöst werden, welche für die verschiedenen Benutzergruppen bewusst gewählt werden sollten. Die Anwendung dieser Aktionen in der App ist in der Bedienungsanleitung "eAccess Mobile - Glutz App", Kapitel "2.4.1 Aktionen" beschrieben.

3.2 Zugriffsrechte

Bevor ein neues Login für einen Mobile User eingerichtet wird, muss ein entsprechendes Rechteprofil vorliegen, welches erlaubt, Smart Access zu verwenden.

Erstellen Sie unter *Einstellungen* → *Zugriffsrechte* eine neue Konfiguration (+) und definieren einen neuen Namen, bspw. 'Smart Access'. Um eAccess Mobile zu nutzen, muss auf *Smart Access* voller Zugriff erteilt werden.

Zugriffsrecht

Name

Smart Access

☐ Mandant Verwalter
 ☒ Spezifische Zugriffsrechte

Alle	Kein Zugriff	Nur lesen	Voller Zugriff
Benutzer	Kein Zugriff	Nur lesen	Voller Zugriff
Benutzer Gruppen Beziehungen	Kein Zugriff		Voller Zugriff
Benutzergruppen	Kein Zugriff	Nur lesen	Voller Zugriff
Medien-Pools	Kein Zugriff	Nur lesen	Voller Zugriff
Medien	Kein Zugriff	Nur lesen	Voller Zugriff
Codes	Kein Zugriff	Nur lesen	Voller Zugriff
Zugangspunkte	Kein Zugriff	Nur lesen	Voller Zugriff
Geräte	Kein Zugriff	Nur lesen	Voller Zugriff
Zugangsberechtigungen	Kein Zugriff	Nur lesen	Voller Zugriff
Smart Access	Kein Zugriff		Voller Zugriff
Fernauslösen	Kein Zugriff		Voller Zugriff
Logs	Kein Zugriff		Voller Zugriff
Software	Kein Zugriff	Nur lesen	Voller Zugriff
Zeitprofile	Kein Zugriff	Nur lesen	Voller Zugriff
Login	Kein Zugriff	Nur lesen	Voller Zugriff
Passwörter lesen	Kein Zugriff		Voller Zugriff

Löschen

Abbildung 2: Zugriffsrecht für Smart Access

3.3 Standort Einstellungen

Ab Software-Version 1.14.0 können speziell für Smart Access GPS-Positionen angelegt werden. Diese Positionen werden für folgende zwei Funktionen verwendet:

- Filterfunktion der Zugangspunkte in der App
- Einschränkung der Fernöffnung in einem bestimmten Radius

Die in diesem Abschnitt beschriebenen Konfigurationen finden Sie im Webclient unter *Einstellungen* → *GPS Positionen*, wie in Abbildung 3 gezeigt.



Abbildung 3: GPS-Positionen einrichten

3.3.1 GPS Positionen

Bevor GPS Positionen verwendet und zugewiesen werden können, müssen diese hier definiert werden. Über die Schaltfläche hinzufügen (+) kann eine neue Position angelegt werden. Der Breiten- und Längen-Grad muss jeweils als Dezimalgrad (WGS84) angegeben werden.

Die Abbildung 4 zeigt ein Beispiel einer Konfiguration. Es gibt drei Möglichkeiten neue Koordinaten zu definieren:

- Manuelle Eingabe der Koordinaten
- Kopieren der Koordinaten über Google Maps und anschliessendes einfügen (ctrl+V) im Feld '*Breiten-grad*'
- Schaltfläche '*Aktuelle Position übernehmen*' auswählen. Die aktuelle Position des Gerätes wird übernommen. Stellen Sie sicher, dass ihr Gerät sich an der Position befindet, welche angelegt werden soll.

Der gewählte Radius wird später verwendet, um die Reichweite für 'Standard GPS Position' und 'Standard Zugangsbereiche' festzulegen. Dazu mehr in den nächsten Abschnitten.



Der gewählte Radius sollte nicht zu knapp gewählt werden, da abhängig vom mobilen Gerät die GPS-Daten, wenn auch nur teilweise, ungenau sein können.

Wichtiger Hinweis: Obwohl hier für Fernauslösen voller Zugriff gewährt wird, ist es dennoch nicht

Abbildung 4: Neue GPS-Position definieren

3.3.2 Standard GPS Positionen

Nachdem die gewünschten GPS-Positionen, wie in Abschnitt 3.3.1 gezeigt, definiert wurden, können diese hier über das '+' Symbol hinzugefügt werden. Die hier hinzugefügten Positionen werden als Filter (*In der Umgebung*) für die App verwendet. Die Funktion in der App ist in der Bedienungsanleitung "eAccess Mobile - Glutz App", Kapitel "2.6 In der Umgebung" beschrieben.

3.3.3 Standard Zugangsbereiche

Nachdem die gewünschten GPS-Positionen, wie in Abschnitt 3.3.1 gezeigt, definiert wurden, können diese hier über das '+' Symbol hinzugefügt werden. Die hier hinzugefügten Positionen sind Berechtigungen im angegebenen Radius. D.h. ausserhalb dieses Bereichs können die Zugangspunkte nicht geöffnet werden. Hier kann zwischen 'Überall' und den erfassten GPS Positionen ausgewählt werden.

3.3.4 Beispiele Setup

Beispiel 1

Die Abbildung 5 zeigt ein Beispiel, wie Mobile User berechtigt sind alle Zugangspunkte (hier von Standort Glutz) von überall aus öffnen können. Zugleich werden die Zugangspunkte in der App unter 'In der Umgebung' im definierten Radius von 100 m angezeigt.

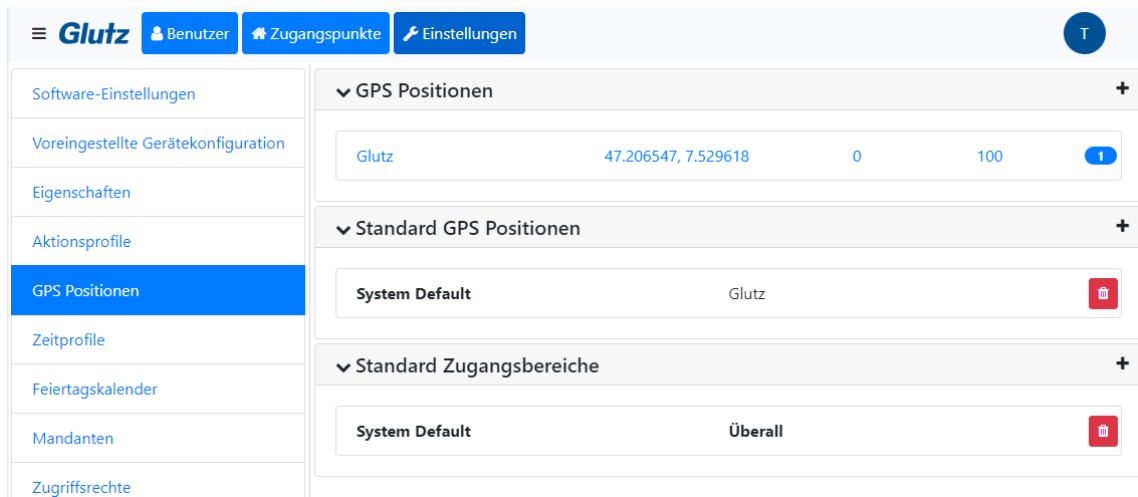


Abbildung 5: GPS Einstellungen Bsp. 1

Beispiel 2

In diesem Beispiel werden die Zugangspunkte in der Glutz App unter 'In der Umgebung' im definierten Radius von 100 m angezeigt. Die Mobile User können jedoch die Zugangspunkte nur im definierten Radius öffnen. Eine Öffnung von ausserhalb ist nicht möglich.

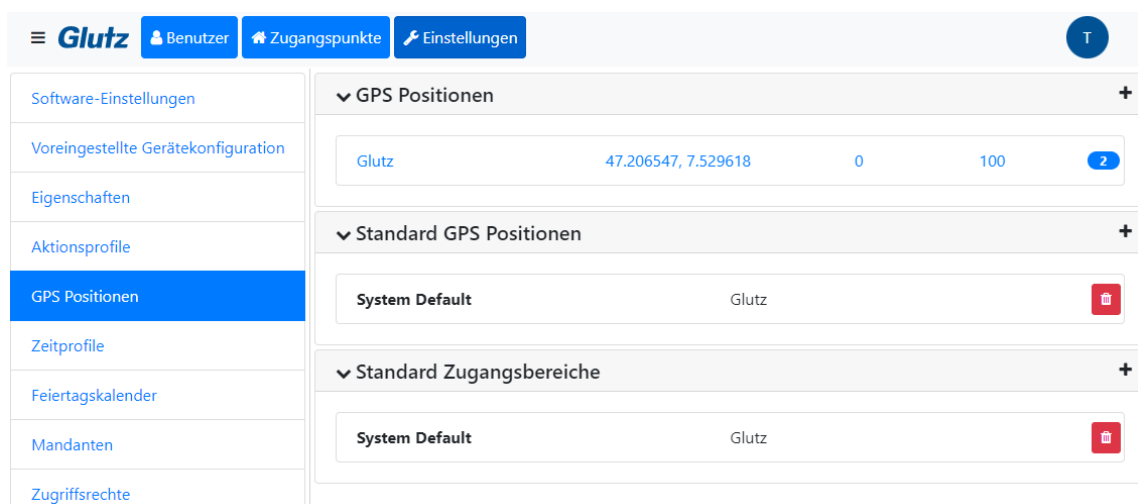


Abbildung 6: GPS Einstellungen Bsp. 2

3.4 System-Informationen für Glutz App vorbereiten

In der Glutz App unter Einstellungen der entsprechenden Instanz können verschiedene Informationen für die Benutzer angezeigt werden.

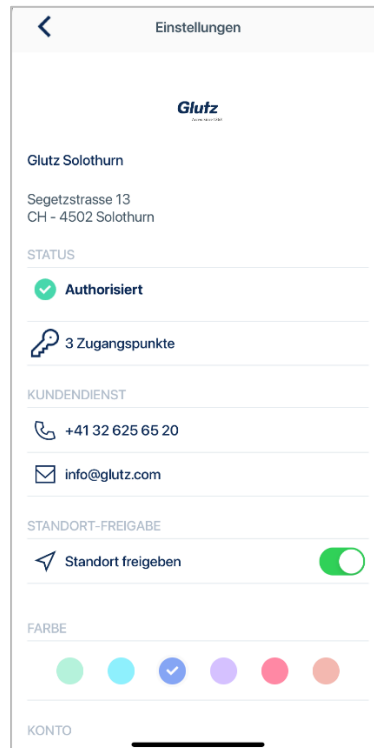


Abbildung 7: Anzeige System-Info

Die Abbildung 7 zeigt ein Beispiel, wie ein Logo, Adressdaten und Kundendienst Informationen angezeigt werden können. Diese Informationen werden im Webclient unter *Einstellungen* bei *System-Informationen* → *Branding* definiert (Abbildung 8).

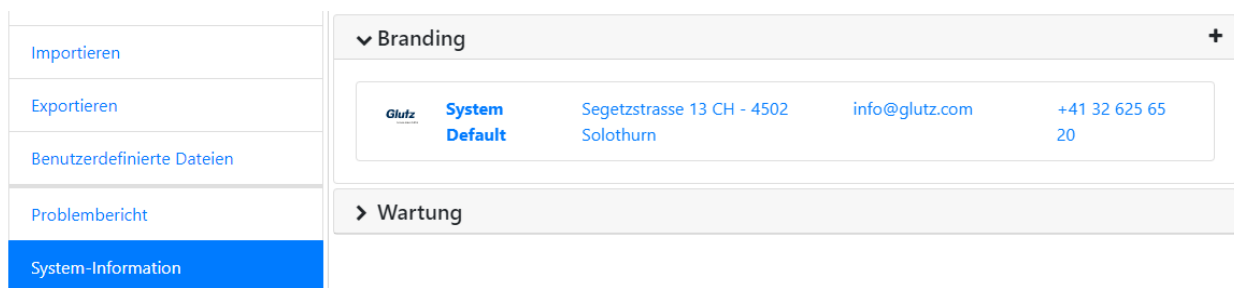
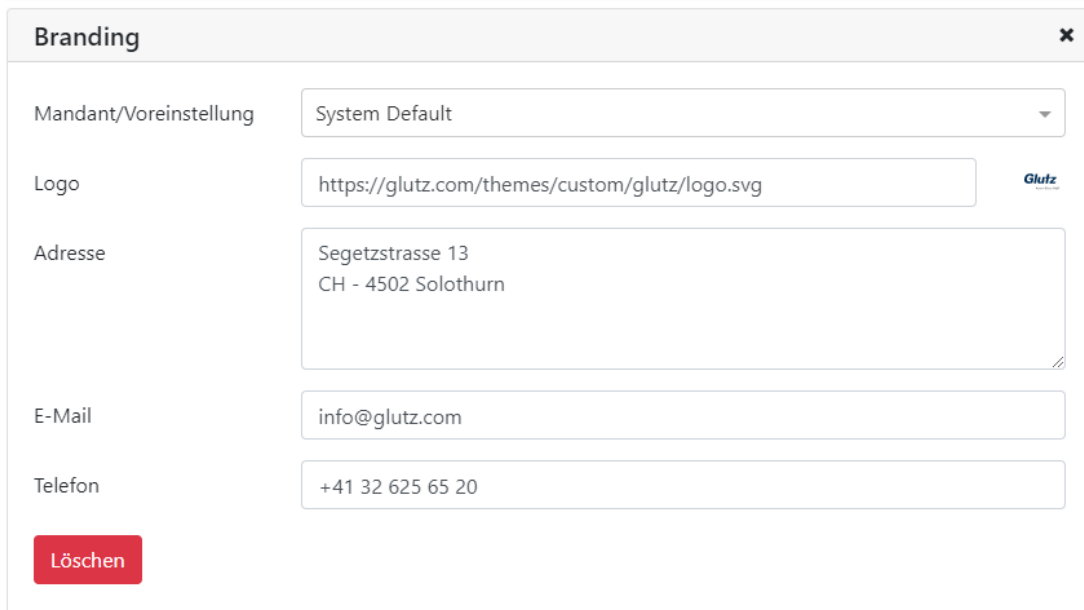


Abbildung 8 : System-Informationen für eAccess Mobile

Es können mehrere so genannte *Brandings* angelegt werden. D.h. diese Informationen können global oder für unterschiedliche Mandanten zugewiesen werden. Dies wird bspw. verwendet, um die Kontaktdaten für den Kundendienst auf die entsprechende Verwaltung zu verweisen.

Weiter kann bei Logo die URL zu einem eigenen Bild definiert werden. Es werden die Formate SVG, PNG und JPEG unterstützt. Die Abbildung 9 zeigt ein Beispiel.



The image shows a web-based configuration form titled "Branding" with a close button (X) in the top right corner. The form contains several input fields and a button:

- Mandant/Voreinstellung:** A dropdown menu with "System Default" selected.
- Logo:** A text input field containing the URL "https://glutz.com/themes/custom/glutz/logo.svg". To the right of the field is a small Glutz logo.
- Adresse:** A text area containing the address "Segetzstrasse 13" and "CH - 4502 Solothurn".
- E-Mail:** A text input field containing "info@glutz.com".
- Telefon:** A text input field containing "+41 32 625 65 20".
- Löschen:** A red button with the text "Löschen" (Delete).

Abbildung 9: Branding Beispiel

3.5 On-Boarding

Nachdem die vorgängig beschriebenen Vorbereitungen abgeschlossen sind, kann den Benutzern eAccess Mobile freigeschaltet werden. Dieser Abschnitt zeigt, wie mit wenigen Klicks ein neuer Mobile User hinzugefügt wird.

3.5.1 Benutzer Smart Access Login erstellen

Wählen Sie dazu unter dem gewünschten Benutzer beim Menu das Smartphone-Icon (*Smart Access Login* hinzufügen) aus, wie in Abbildung 10 gezeigt.

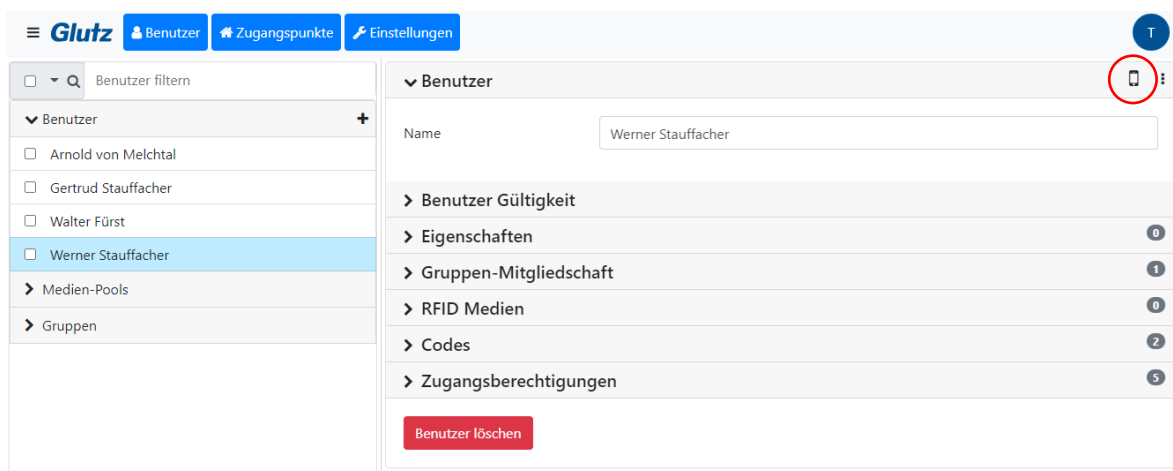


Abbildung 10: Smart Access Login einem Benutzer zuweisen

Anschließend öffnet sich die Konfiguration für das entsprechende Login, wobei die meisten Einstellungen vorkonfiguriert sind. Geben Sie die E-Mail-Adresse des Benutzers und dessen gewünschte Sprache ein, wie in Abbildung 11 gezeigt.

Smart Access Login hinzufügen

Benutzer: Werner Stauffacher

Benutzername: Werner Stauffacher

E-Mail: werner.stauffacher@glutz.com

Sprache: Deutsch

Optionen: ☒ Nur von der App generierte Passwörter zulassen

Zugriffsrecht: eAccess Mobile

Mandant: Alle

Aktionsprofil: Default

Einladung versenden / Verfallszeit: ☒ 2 Tage

Abbildung 11: Smart Access Login konfigurieren

Bei der Konfiguration (Abbildung 11) können optional noch weitere Einstellungen vorgenommen werden:

Benutzer

Der Benutzer, für welchen eAccess Mobile freigeschaltet werden soll. Diese Einstellung kann nicht überschrieben werden, da diese geöffnete Konfiguration schon bei der Auswahl des Benutzers definiert wird (Abbildung 10).

Benutzername

Dies ist der Benutzername, welcher für das zu erstellende Login verwendet und unter *Einstellungen* → *Logins* angezeigt werden soll. Meistens entspricht dies dem Benutzer-Namen und muss nicht geändert werden.

E-Mail

Die E-Mail-Adresse des Benutzers, auf welche die Einladung für die Registrierung gesendet werden soll.

Sprache

Die Sprache, in welcher der Einladungslink versendet wird.

Optionen – Von der App generierte Passwörter

Ist diese Option angewählt, wird die App automatisch ein sicheres Passwort für den Benutzer generieren (Abbildung 12). Dies ist die schnellere und auch sicherere Variante für die Anmeldung von Mobile User. Passwörter werden verschlüsselt auf dem Gerät gespeichert und können nur von der Glutz App entschlüsselt werden. Auf beiden Plattformen, auf Android sowohl auch auf iOS, kann dieser sichere Speicher mit dem Android- bzw. iOS-Konto synchronisiert werden. Ist diese Synchronisierung auf dem Smartphone ausgeschaltet, muss für diese Person bei einem Smartphone-Wechsel über den Webclient eine erneute Einladung gesendet werden. Wie dies funktioniert, wird in Abschnitt 0 erklärt.

The screenshot shows the Glutz eAccess login interface. At the top, there are links for 'Anmelden' and 'Abbrechen'. The Glutz eAccess logo is centered. Below the logo, there are two input fields: the first contains the URL 'https://ecsnk1ne.eaccess.glutz.com' and the second contains the email 'werner.stauffacher@glutz.com'. At the bottom, there is a dark blue button labeled 'ANMELDEN'.

Abbildung 12: Automatisches Passwort

Wenn diese Option nicht angewählt ist, kann der Benutzer ein eigenes Passwort festlegen (Abbildung 13). Der Benutzer kann so auch bei einem Geräte-Wechsel sich selbständig wieder einloggen, vorausgesetzt er kennt den Systemnamen der Anlage.

The screenshot shows the Glutz eAccess login interface for manual password entry. It includes the same top links and logo as the previous screen. Below the logo, there are four input fields: the first contains the URL 'https://ecsnk1ne.eaccess.glutz.com', the second contains the email 'werner.stauffacher@glutz.com', the third is labeled 'Neues Passwort', and the fourth is labeled 'Neues Passwort bestätigen'. Below these fields, there is a small text block: 'Das neue Passwort muss mind. 8 Zeichen lang sein, aus Gross- und Kleinbuchstaben sowie Sonderzeichen bestehen und in keinem Wörterbuch zu finden sein oder mit Ihnen in Verbindung stehen.' At the bottom, there is a grey button labeled 'ANMELDEN'.

Abbildung 13 : App Login mit Benutzer-Passwort



Verwenden Sie, wenn möglich, automatisch generierte Passwörter, da diese erheblich sicherer sind als manuell erstellte Passwörter.

Zugriffsrecht

Hier kann das gewünschte Zugriffsrecht für Smart Access ausgewählt werden. Dies ist in Abschnitt 3.2 genauer erklärt. Diese Einstellung wird automatisch ausgefüllt.

Mandant

Hier kann der gewünschte Mandant ausgewählt werden, in welchem der Benutzer zugewiesen ist.

Aktionsprofil

Dies ist das entsprechende Aktionsprofil, welches in Abschnitt 3.1 genauer beschrieben ist.

Einladung versenden / Verfallszeit

Ist diese Einstellung ausgewählt (default), wird nach Abschliessen des Formulars, dem Benutzer direkt die Einladungs-Mail versendet. Zusätzlich kann noch die Verfallszeit, also die Gültigkeitsdauer des Einladungs-Links in der E-Mail bestimmt werden. Wir empfehlen die Voreinstellung der Verfallszeit zu verwenden.

3.5.2 Benutzer kontaktieren

Nachdem einem Benutzer ein Smart Access Login zugewiesen wurde, werden ihm neue Funktionen freigeschaltet (Abbildung 14). Es wird neu das 'Smart Access Profil' angezeigt, welches hier auch angepasst werden kann, wenn bspw. ein Benutzer andere Spezial Aktionen auslösen kann.

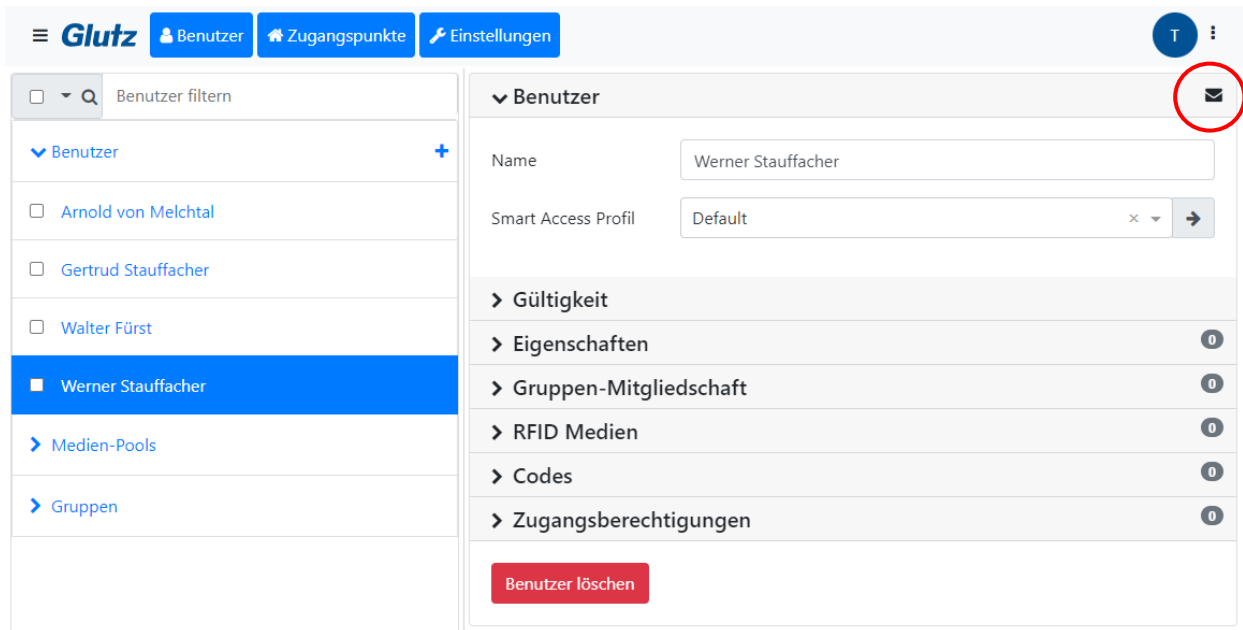


Abbildung 14 : Benutzer mit Smart Access Login

Weiter erscheint beim Benutzer ein E-Mail-Icon, womit der Benutzer schnell und einfach kontaktiert werden kann. Mit einem Klick auf dieses Icon erscheinen drei weitere Funktionen:

App Einladung

Mit einem Klick wird dem Benutzer eine neue Einladung per Mail zugestellt.

Passwort zurücksetzen

Der Benutzer erhält eine E-Mail mit einem Link, mit welchem dieser sein Passwort neu definieren kann. Diese Funktion erscheint nicht, wenn bei der Smart-Access Einladung nur von der App generierte Passwörter zugelassen sind (siehe Abschnitt 3.5.1).

E-Mail

Die Standard-Mail Applikation wird gestartet (bspw. Outlook) und dem Benutzer kann schnell eine persönliche Nachricht geschickt werden.

4. Bekannte Fehler

Da mehrere tausend verschiedene Smartphone-Modelle auf dem Markt verfügbar sind und jeder Benutzer andere Apps und Versionen installiert haben kann, ist es nicht ausgeschlossen, dass Fehlfunktionen auftreten können. Leider können wir darauf nur beschränkt Einfluss nehmen. Durch die stetige Weiterentwicklung versuchen wir so weit als möglich diese Fehler zu beheben.

Dieser Abschnitt erläutert Fehler, welche uns bekannt sind, auf welche wir jedoch keinen Einfluss nehmen können.

4.1 On-Boarding

4.1.1 Einladungs-Link funktioniert nicht

Problem: Der Einladungslink, welcher per Mail zugestellt wurde, funktioniert nicht, bzw. die App öffnet sich nicht.

Bekannte Ursache: Der verwendete Browser auf dem Smartphone öffnet standardmässig ein Inkognitofenster (privates Surfen), bei welchem die Funktionen nicht verwendet werden können. Durch unsere Sicherheitsmechanismen kann es sein, dass der Browser gewisse Daten nicht bearbeiten lässt.

Lösung: Öffnen Sie den Einladungslink in einem normalen Fenster oder Tab. Deaktivieren Sie ggf. das private Surfen unter den Einstellungen in Ihrem Browser.

Bekannte Ursache (iPhone): Auf iOS beim Safari Browser kann es vorkommen, dass wenn die Funktion 'Prevent Cross-Site Tracking' aktiv ist, der Einladungslink nicht geöffnet werden kann.

Lösung: Deaktivieren Sie vor dem Öffnen des Einladungslinks unter den Safari-Einstellungen die Funktion 'Prevent Cross-Site Tracking':

