

Solothurn, 07.09.2022

Webclient Release 1.14.0

eAccess Kurzanleitung neue Funktionen

Index V1.0
Doc-Nr. MA-10167

Glutz AG, Solothurn

Inhaltsverzeichnis

1.	Einleitung	2
2.	Änderungen Benutzer und Gruppen	3
2.1	Darstellung	3
2.2	Klonen	3
3.	Änderungen Zugangspunkte und Geräte	5
3.1	Umbenennen der Gebäudestruktur	5
4.	eAccess Mobile	6
4.1	Integration PFA	6
4.2	Benutzer Gültigkeiten	6
4.3	Branding	6
4.4	GPS Positionen	6
5.	Validierung der Lizenzen	7
6.	Zwei-Faktor-Authentisierung	7
7.	Login-Verwaltung	9
7.1	Filterfunktion	9
7.2	Login aktivieren/deaktivieren	9
8.	Logdaten	9
9.	Einsicht in das Systemprotokoll	9

1. Einleitung

Beim neuen Release 1.14.0 wurden einige Neuerungen zur Bedienung, aber auch Verbesserungen bei der Performance und Stabilität eingeführt. Dieses Dokument zeigt die neuen Funktionen, welche Sie als Anwender neu verwenden können.

Neben den Neuerungen der Oberfläche im Webclient wurden auch viele Optimierungen im Backend eingeführt. Eine vollständige Liste der Neuerungen finden Sie auf unserer [Changelog-Seite](#).

2. Änderungen Benutzer und Gruppen

2.1 Darstellung

Bei den Benutzern wurde die Darstellung optimiert. So ist nun die Durchgängigkeit der Ansichten zwischen den Zugangspunkten und den Benutzern, sowie auch den Gruppen und Medien-Pools gewährleistet und angenehmer in der Benutzung.

2.2 Klonen

Neu in der Webclient Version 1.14.0 können Benutzer und auch Gruppen geklont werden. D.h. wenn neue aber sehr ähnlich zu bestehenden Benutzer oder Gruppen erstellt werden möchten, können diese ganz einfach dupliziert werden.

Die Abbildung 1 zeigt wie Sie einen Benutzer klonen können. Wählen Sie dazu den zu duplizierenden Benutzer aus und wählen oben rechts unter dem Menu 'Benutzer klonen' aus.

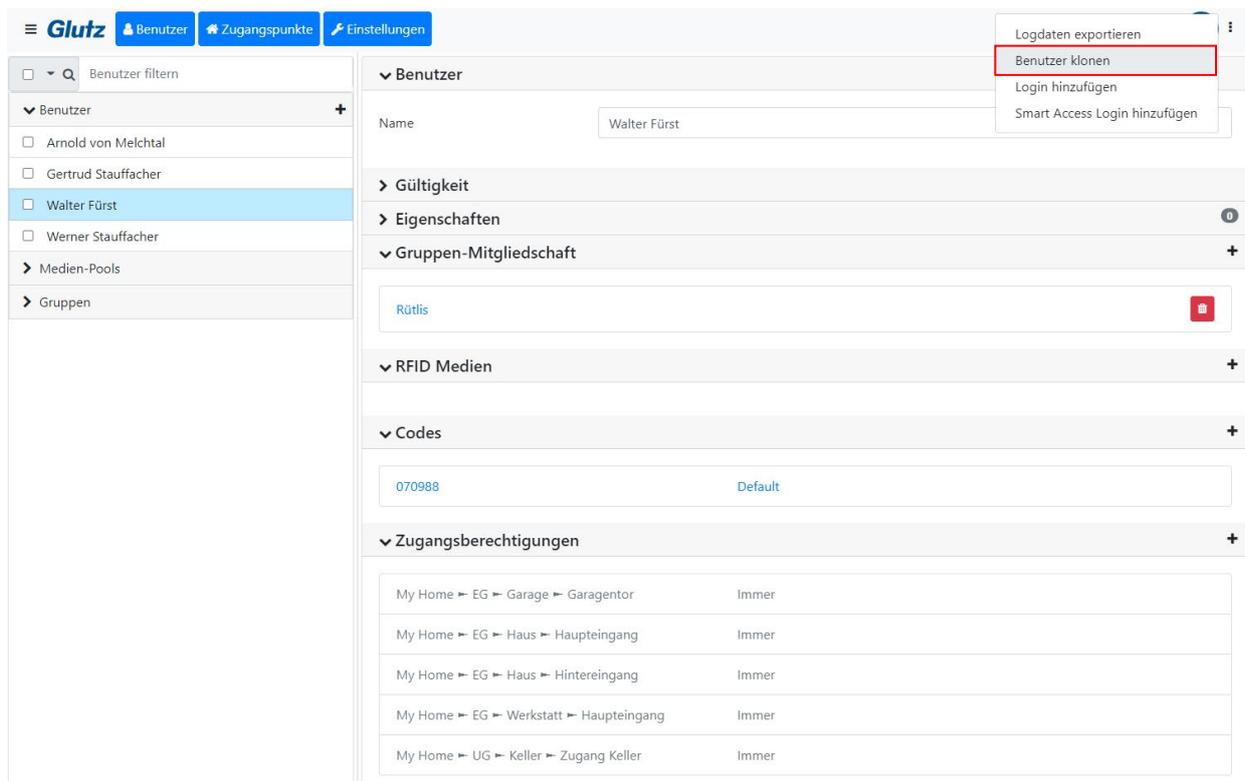


Abbildung 1 : Benutzer klonen

Daraufhin öffnet sich der Dialog, wo der Name für den zu erstellenden Benutzer definiert werden kann. Mit dem geklonten Benutzer können auch mehrere Benutzer gleichzeitig erstellt werden, wie in Abbildung 2 gezeigt

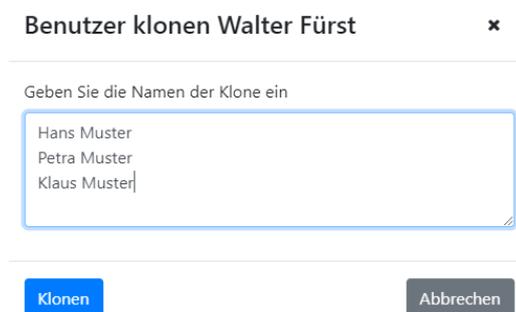


Abbildung 2 : Mehrere Benutzer gleichzeitig erstellen

Wählen Sie dann 'Klonen' aus, um die Benutzer der Anlage hinzuzufügen. Anschliessend erscheinen die Benutzer in der Übersicht und haben die gleichen Zutrittsrechte wie der ausgewählte Benutzer (Abbildung 3).

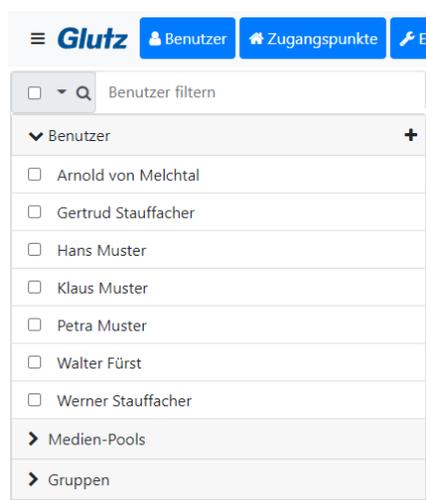


Abbildung 3 : Geklonte Benutzer erstellt

Der gleiche Vorgang kann mit den Gruppen gemacht werden. Wichtig bei beiden Vorgängen ist, dass nicht alle Parameter kopiert werden. Hier eine kurze Übersicht, was nicht vom entsprechenden Klon übernommen wird:

- Benutzer
 - o RFID Medien
 - o Codes
- Gruppe
 - o Eigenschaften
 - o Benutzer (Personen)

Alle nicht gelisteten Daten werden vom geklonten Benutzer kopiert.

3. Änderungen Zugangspunkte und Geräte

3.1 Umbenennen der Gebäudestruktur

Neu können die Hierarchien (Eigenschaften) für Zugangspunkte ganz einfach gruppiert umbenannt werden, ohne dass jeder Zugangspunkt einzeln geändert werden muss.

Wenn bspw. ein Stockwerk umbenannt werden soll, wählen Sie den top-level Eintrag dieser Gruppe und benennen Sie dort die Bezeichnung um. In Abbildung 4 wird gezeigt, wie das Stockwerk 'EG' in 'OG' umbenannt wird. Nach Bestätigung der Änderung werden alle Zugangspunkte, welche unter dem Stockwerk 'EG' gelistet waren, neu unter 'OG' zu finden sein.

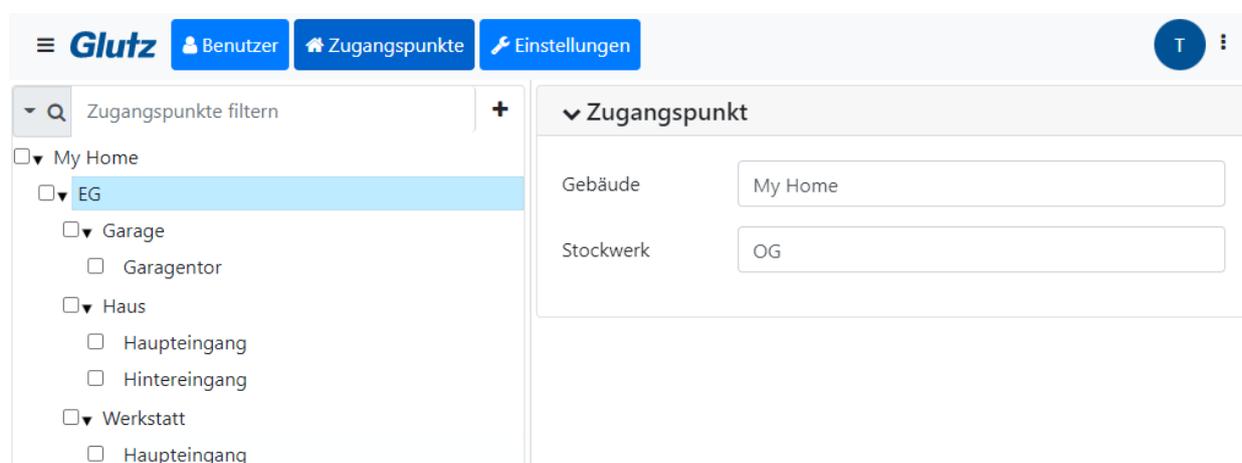


Abbildung 4 : Umbenennen von Hierarchien

Sie können auch nur einzelne Zugangspunkte anwählen und dort die Eigenschaften umbenennen, um zum Beispiel einen Zugangspunkt in eine andere Gruppe (oder im gezeigten Beispiel: anderes Stockwerk) zu verschieben.

4. eAccess Mobile

Ab dem Release 1.14.0 kann eAccess mit eAccess Mobile benutzt werden. Die neue Glutz-App finden Sie in den entsprechenden App-Stores für iOS und Android.

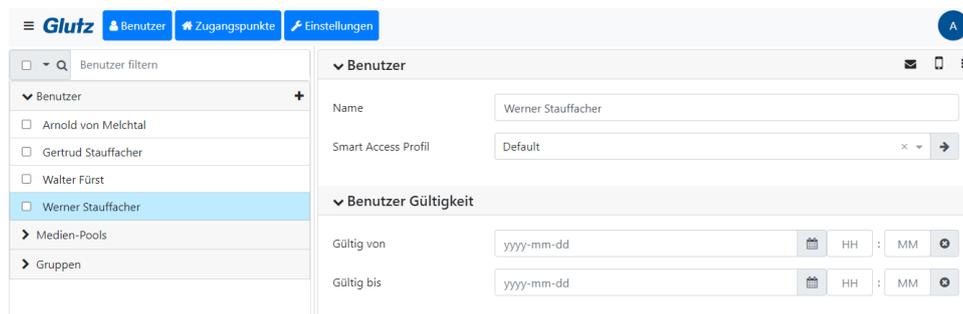
Wie eAccess Mobile (Smart-Access) eingerichtet und benutzt wird und wie die App aufgebaut und bedient wird, können Sie den separaten Anleitungen MA-10165 und MA-10166 entnehmen.

4.1 Integration PFA

eAccess Mobile kann zukünftig auch für Paketfachanlagen verwendet werden und ist in Version 1.14.0 auch schon vorbereitet. In einem zweiten Schritt folgt das Update der Integration für den Access Controller. Beim Release der neuen Version von gasync (PFA Schnittstelle) werden wir Sie informieren.

4.2 Benutzer Gültigkeiten

Neu im Zusammenhang mit eAccess Mobile kann die Gültigkeit für einen Benutzer definiert werden, wie in Abbildung 5 gezeigt.



The screenshot shows the Glutz web interface. At the top, there are navigation tabs: 'Benutzer', 'Zugangspunkte', and 'Einstellungen'. The main content area is divided into two sections. On the left, there is a sidebar with a search bar and a list of users under the heading 'Benutzer'. The user 'Werner Stauffacher' is selected and highlighted. On the right, the settings for 'Werner Stauffacher' are displayed. The 'Benutzer Gültigkeit' section is expanded, showing two date pickers: 'Gültig von' and 'Gültig bis'. Each date picker has a calendar icon and a time selection dropdown with options for HH and MM.

Abbildung 5 : Benutzer Gültigkeit

Benutzen Sie diese Funktion, um temporäre Zugangsberechtigung für einen Benutzer zu erteilen, ohne dass der Benutzer gelöscht werden muss. So bleiben die Einstellungen und Daten des entsprechenden Benutzers erhalten, um diesem die Zugangsberechtigungen später schnell wieder zu aktivieren.

4.3 Branding

Unter *Einstellungen* → *System-Informationen* → *Branding* können neue Kontaktdaten und Adresse des Betreibers oder Support eingefügt werden. Wie dies eingerichtet wird und welchen Zweck dies hat, wird in der Bedienungsanleitung zu eAccess Mobile (MA-10165) im Detail erklärt.

4.4 GPS Positionen

Bei den Einstellungen gibt es ab Software Version 1.14.0 die Möglichkeit GPS Positionen zu verwalten. Dies wird ausschließlich für eAccess Mobile verwendet und wird in der Bedienungsanleitung (MA-10165) ausführlich erklärt.

5. Validierung der Lizenzen

Durch das neue Lizenzmodell, welches wir im Sommer 2022 eingeführt haben, werden ab Version 1.14.0 die Lizenzen genauer validiert. Beispielsweise werden die Anzahl gelöster Zugangspunkte im System kontrolliert und auch deren Ablaufdatum.



Wichtiger Hinweis: Es kann sein, dass Sie in Ihrer Anlage bisher Module verwenden, welche die gekaufte bzw. gelöste Lizenz überschreitet. Ist dies der Fall, können Sie keine Mutationen an der Anlage mehr vornehmen. Kontaktieren Sie Ihren Ansprechpartner und passen Sie ggf. die Lizenzen an das System an.

Sie haben die Möglichkeit unter der URL <https://cloud.eaccess.glutz.com/anlage-name/licenses> die Lizenzen und deren Status abzufragen.

Sie können dies auch im Webclient unter Einstellungen → System-Informationen einsehen.

6. Zwei-Faktor-Authentisierung

Neu gibt es beim eAccess Webclient die Möglichkeit, dass sich ein Benutzer mit Zwei-Faktor Authentisierung anmelden muss. Dies erhöht die Sicherheit beim Zugriff auf die Datenbank. Dazu legen Sie wie gewohnt ein neues Login an. Bei den Einstellungen sind nun zwei weitere Optionen, wie in Abbildung 6 gezeigt.

The screenshot shows the 'Einloggen' (Login) configuration page in the Glutz webclient. The left sidebar contains a menu with 'Logins' selected. The main content area is titled 'Einloggen' and contains several input fields: 'Benutzername' (Werner Stauffacher), 'Benutzer' (Werner Stauffacher), 'E-Mail' (werner.stauffacher@glutz.com), 'Sprache' (Deutsch), and 'Beschreibung'. Under the 'Optionen' section, there are three checkboxes: 'Login aktiv' (checked), 'Nur von der App generierte Passwörter zulassen' (unchecked), and 'Zwei-Faktor-Authentisierung erforderlich' (checked). Below these is a dropdown menu for 'Zwei-Faktor-Authentisierung Intervall' set to '2 Tage'. At the bottom, there are fields for 'Neues Passwort' and 'Passwort bestätigen', both masked with dots.

Abbildung 6 : Zwei-Faktor-Authentisierung einschalten

Aktivieren Sie die Checkbox 'Zwei-Faktor-Authentisierung erforderlich' und stellen Sie das gewünschte Intervall zur erneuten Authentisierung ein. Als Default und Empfehlung sind 2 Tage vordefiniert.

Wenn sich der neue Benutzer nun mit seinem Login anmeldet, erscheint die entsprechende Seite für die Zwei-Faktor-Authentisierung (Abbildung 7).

Wie auch auf der Seite für die Einrichtung beschrieben ist, wird eine Authenticator-App, welche TOTP (Time-Based One-Time-Password) unterstützt, benötigt. Installieren Sie bspw. die App 'Google Authenticator' und scannen Sie den QR-Code mit der Kamera Ihres Smartphones. Anschliessend erscheint in der App ein 6-stelliger Code, welchen Sie in das Feld zur Prüfung eingeben. Mit einem Klick auf 'Zwei Faktor prüfen' wird der Prozess abgeschlossen.

Glutz eAccess Multi-Faktor-Authentisierung

Zwei-Faktor-Authentisierung für Ihr Login einrichten.



Für Ihr Login ist eine Zwei-Faktor-Authentifizierung erforderlich. Dazu benötigen Sie eine Zwei-Faktor-Authentifizierungs-App auf Ihrem Smartphone, welche TOTP unterstützt, wie z.B. "Twilio Authy" oder "Google Authenticator". Richten Sie in dieser App mit Hilfe des QR-Codes ein Konto ein. Falls der QR-Code nicht verwendet werden kann, dann verwenden Sie bitte den folgenden Code:

BALE JRFM UQJ4 J2ZP A5YI PWHA BNY6 CDVK

Geben Sie bitte nach der Einrichtung Ihres Kontos den aktuell gültigen Code zur Bestätigung in das untenstehende Eingabefeld ein. Bitte beachten Sie, dass sich die Kontodaten solange ändern können, bis Sie diese zum ersten Mal verifiziert haben. Danach ist dieses Konto für das Login zwingend erforderlich.

Verifizieren Sie Ihr Login mit Ihrem zweiten Faktor.

Bitte geben Sie den aktuellen zeitabhängigen Code von Ihrem Smartphone ein und klicken Sie auf "Zweiten Faktor prüfen".

Abbildung 7 : Zwei-Faktor-Authentisierung einrichten

Nach dem eingestellten Intervall von Abbildung 6 muss dieser Prozess wiederholt werden.



Wichtiger Hinweis: Personen, welche Zwei-Faktor-Authentisierung bei ihrem Login aktiv haben, müssen bei Benutzung von eAccess Mobile ein getrenntes Login haben.

7. Login-Verwaltung

7.1 Filterfunktion

Eine neue Filterfunktion bei *Einstellungen* → *Logins* hilft eine noch bessere Übersicht über die Logins zu erhalten. Klicken Sie dazu auf die entsprechenden Icons:

Systemverwalter, Login aktiv, Zwei-Faktor-Authentisierung, Smart-Access (von Links auf Abbildung 8)



Abbildung 8 : Filter Logins

Bei einem Klick auf den gewünschten Filter erscheint das Icon blau. Dies bedeutet, dass alle Logins von bspw. Smart-Access angezeigt werden. Bei einem erneuten Klick auf das gleiche Icon, erscheint dieses rot. So werden alle Logins angezeigt, welche nicht ein Smart-Access Login sind.

7.2 Login aktivieren/deaktivieren

Die Logins können manuell aktiviert oder deaktiviert werden, ohne diese zu Löschen. Dies ist dann hilfreich, wenn das Login später erneut benutzt und temporär deaktiviert werden soll. Auf Abbildung 6 sehen Sie diese Einstellung unter *Optionen*.

8. Logdaten

Ab Version 1.14.0 werden Öffnungen, welche über die Software getätigt werden, im Gerätelog angezeigt.

9. Einsicht in das Systemprotokoll

Für Experten kann neu der top-level Systemadministrator das Systemprotokoll der gesamten Anlage einsehen und nachverfolgen. Das Systemprotokoll kann mit der URL <https://cloud.eaccess.glutz.com/anlage-name/settings/systemlog> angezeigt werden. Diese Funktion ist nicht für Endkunden gedacht.