



# Anleitung VOTING: Adminpanel

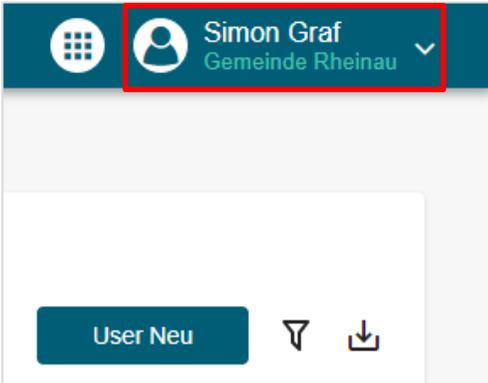
Stand 05.09.2024

1	Verwaltung von Usern	1
2	Berechtigungskonzept: Übersicht Rollen	5

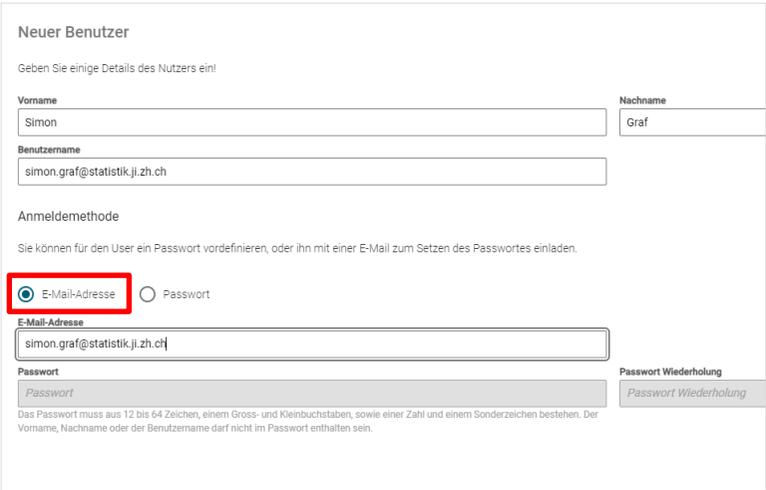
## 1 Verwaltung von Usern

Nr.	Schritt	Prozessbeschreibung	Screen/Dokumente/zu beachten
1)	Login MyAccount	<p>Einstieg in MyAccount via:</p> <p><a href="https://abraxas-vo.sec.abraxas-apps.ch/myaccount/">https://abraxas-vo.sec.abraxas-apps.ch/myaccount/</a></p> <p>Anmeldung mit Benutzername (E-Mail-Adresse), Passwort und 2-Faktor-Authentifizierung (siehe entsprechende <a href="#">Anleitung für das Einrichten des 2. Faktors via Abraxas SECURE Access</a>)</p>	
2)	Adminpanel öffnen	<p>In der Übersicht von MyAccount die Applikation SECURE Connect Adminpanel aufrufen → Die Applikation öffnet sich in einem neuen Tab. Alternativ kann das Adminpanel auch direkt über die URL <a href="https://abraxas-vo.sec.abraxas-apps.ch/adminpanel/">https://abraxas-vo.sec.abraxas-apps.ch/adminpanel/</a> aufgerufen werden.</p> <p>Falls mehrere Mandanten zur Verfügung stehen, sicherstellen, dass der korrekte Mandant gewählt ist. Dazu kann mit einem Klick auf den eigenen Username in der Kopfzeile oben rechts am Bildschirm der Mandant gewechselt werden (sofern mehrere Mandanten zur Verfügung stehen).</p>	



Nr.	Schritt	Prozessbeschreibung	Screen/Dokumente/zu beachten
			
3)	Eigene Berechtigungen prüfen	<p>Mit einem Klick auf das Tab «Mein Account» können die eigenen Angaben und Berechtigungen eingesehen und angepasst werden.</p> <p>Für die nachfolgenden Schritte wird für die Applikation «Adminpanel» die Berechtigung «Admin» benötigt (siehe Rollenkonzept im Kapitel 2).</p>	

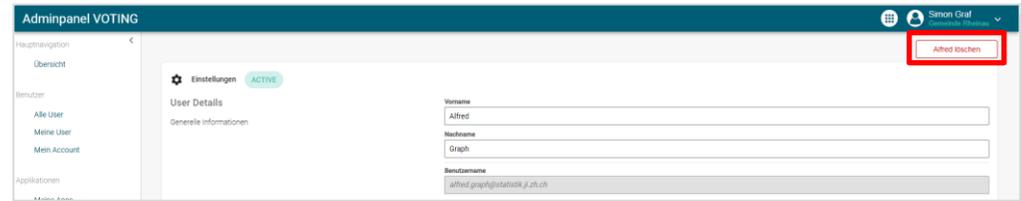


Nr.	Schritt	Prozessbeschreibung	Screen/Dokumente/zu beachten
4)	Neuen User hinzufügen	<p>In den Tabs «Übersicht» oder «Meine User» kann ein oder eine Admin (Zugewiesene Berechtigung Admin für die Applikation Adminpanel, siehe Berechtigungskonzept in Kapitel 2) neue Benutzer für den offenen Mandaten anlegen. Dafür wird oben rechts der Button «User Neu» geklickt.</p> <p>Im sich öffnenden Pop-Up wird der Vorname, der Name, der Username und die E-Mail-Adresse abgefüllt.</p> <p>Anschliessend mit «OK» abschliessen.</p> <p>Der User erscheint nun in der Übersicht (und bei «Meine User»).</p> <p><b><u>Einrichten seitens User</u></b></p> <p>Gleichzeitig erhält die Benutzerin ein E-Mail mit einem Link. Mit diesem Link muss innert 72 Stunden ein Passwort gesetzt werden.</p> <p>Anschliessend muss der neue Benutzer beim ersten Login einen angezeigten QR-Code mit der mobilen Applikation «Ab-raxas SECURE Access» scannen und damit den zweiten Faktor für das Login einrichten.</p>	 <p><b>Wichtig:</b></p> <ul style="list-style-type: none"> <li>Um eine eindeutige Zuordnung des Users zu gewährleisten, <b>immer die E-Mail-Adresse als Username verwenden!</b></li> <li>Bei der Anmeldemethode <b>immer die Option «E-Mail-Adresse» wählen! User ohne hinterlegte E-Mail-Adresse werden gelöscht.</b> Dabei darf es sich bei Personen ohne offizielle E-Mail-Adresse natürlich auch um private E-Mail-Adressen handeln.</li> </ul>
5)	Usern neue Berechtigungen erteilen (d. h. Berechtigungen auf neuer Applikationen hinzufügen)	<p>Neu erstellte User haben keine Berechtigungen (ausser «User» in der Applikation «MyAccount»). Damit sie beispielsweise eine Abstimmung einrichten oder Ergebnisse eintragen können, müssen ihnen Berechtigungen auf den entsprechenden Applikationen gegeben werden.</p> <p><b><u>Berechtigung für neue Applikation hinzufügen</u></b></p> <p>Dazu wählt man einen User z. B. im Tab «Übersicht» mit einem Doppelklick aus.</p>	



Nr.	Schritt	Prozessbeschreibung	Screen/Dokumente/zu beachten
		<p>In der zweiten Kachel «Berechtigungen» sind jetzt alle Berechtigungen des Users auf allen Applikationen sichtbar. Mit einem Klick auf «Berechtigung hinzufügen» öffnet sich ein Pop-Up.</p> <p>Die Felder «User» und «Mandant» sollten jetzt schon korrekt abgefüllt sein. Anschliessend eine Applikation wählen und eine Rolle zuteilen.</p> <p>Die Berechtigungen der zugeteilten Rollen werden kumuliert, das heisst, es stehen die Rechte aller Rollen zur Verfügung, die zugeteilt sind.</p>	<div data-bbox="1102 352 1711 847"> </div> <p><b>Wichtig:</b></p> <ul style="list-style-type: none"> <li>• Es dürfen <b>keine Berechtigungen auf den UAT-Applikationen</b> zugeteilt werden. Die UAT-Umgebung (User Acceptance Test) ist nur für das Testen von neuen VOTING-Funktionen relevant. <b>Berechtig Sie Ihre User nur auf den ZH VOTING-Applikationen!</b></li> <li>• Es werden <b>nur Applikationen angezeigt, auf denen ein User noch keine Berechtigungen hat!</b> Wenn also eine Applikation fehlt, muss geprüft werden, ob bereits eine Berechtigung existiert (siehe nachfolgend Schritt 5).</li> </ul>
6)	Bestehende Berechtigungen anpassen	<p>Falls ein User auf einer Applikation schon berechtigt ist (und die Berechtigung entsprechend auf der Berechtigungsübersicht des Users (Zugriff via Doppelklick auf den User im Tab «Alle User») angezeigt wird, kann die Berechtigung auch direkt da angepasst werden. Dazu einfach die neue Rolle mittels Drop-Down-Menu auswählen und rechts auf das Speichern-Symbol klicken.</p>	<div data-bbox="1102 1145 2123 1401"> </div> <p><b>Wichtig:</b></p>



Nr.	Schritt	Prozessbeschreibung	Screen/Dokumente/zu beachten
			Die neue Rolle unbedingt mit dem Speichern-Symbol bestätigen.
7)	User löschen	Mit einem Doppelklick auf die Benutzerin (z. B. via Tab «Alle User») gelangt man auf das Profil der Benutzerin. Um den User zu löschen, kann oben rechts der Button «VORNAME löschen» geklickt werden. Anschliessend im Pop-Up mit dem Button «löschen» bestätigen.	 <p><b>Wichtig:</b> Nach einem Jahr Inaktivität wird ein User automatisch gelöscht und muss bei Bedarf wieder neu angelegt werden.</p>

## 2 Berechtigungskonzept: Übersicht Rollen

Nr.	Applikation	Rolle	Beschreibung
1)	<u>MyAccount</u>	User	Hat Zugriff zu MyAccount. Berechtigung wird automatisch vergeben, sobald ein User erstellt wird.
2)	<u>SECURE Access</u>	TenantReader	Kann im Adminpanel alle Informationen des Mandanten (d. h. der Gemeinde) einsehen
3)	Zugriff auf SECURE Access gibt einem User Lese- und Bearbeitungsrechte für Informationen im Adminpanel. Dies ist nur für Gemeindeadmins nötig.	TenantManager	Kann im Adminpanel alle Informationen des Mandanten (d. h. der Gemeinde) einsehen und Benutzer und Berechtigungen bearbeiten.
4)		Function_TenantManagerAssigner	Kann im Adminpanel alle Informationen des Mandanten (d. h. der Gemeinde) einsehen und Benutzer und Berechtigungen bearbeiten. Ausserdem kann diese Rolle anderen Personen die Rolle TenantManager erteilen.
5)		Function_TransactionConfirmation	Diese Rollen sind für Gemeinden nicht relevant und können nicht vergeben werden.
6)		SystemAdmin	
7)		SystemManager	
8)		SystemReader	
9)		TenantAdmin	
10)	<u>SECURE Connect Adminpanel</u>	Admin	Kann User erstellen, berechtigen und löschen (nur in Verbindung mit SECURE Access Berechtigung)



Nr.	Applikation	Rolle	Beschreibung
11)	Zugriff auf das Adminpanel ist nur für Gemeindeadmins nötig.	Berechtigungsverwalter	Kann User berechtigen (nur in Verbindung mit SECURE Access Berechtigung)
12)		User	Kann eigenen Account einsehen (nur in Verbindung mit SECURE Access Berechtigung)
13)	<b><u>ZH VOTING Basis</u></b>	Wahlverwalter	Kann Wahlen und Abstimmungen für Wahlkreise des Mandanten zu bestehenden Urnengängen hinzufügen und neue Urnengänge eröffnen.
14)	Zugriff auf ZH VOTING Basis ist nur für Personen notwendig, die Geschäfte eröffnen oder bearbeiten.	Wahlunterstützer	Kann Wahlen und Abstimmungen für Wahlkreise des Mandanten zu bestehenden Urnengängen hinzufügen.
15)	<b><u>ZH VOTING Ausmittlung Erfassung</u></b>	Wahlverwalter	Kann alle nötigen Manipulationen für die Eingabe und die Übermittlung der Resultate vornehmen.
16)		Wahlunterstützer	Hat dieselben Möglichkeiten wie der Wahlverwalter ausser: <ul style="list-style-type: none"><li>• Erfassungsweise festlegen</li><li>• Ergebnisse übermitteln</li></ul>
17)		Erfasser	Kann Bunde und Wahlzettel erfassen und die Bundkontrolle durchführen.
18)		Erfasser ohne Bundkontrolle	Kann Bunde und Wahlzettel erfassen.
19)		Bundkontrolleur	Kann die Bundkontrolle durchführen.
20)	<b><u>ZH VOTING Ausmittlung Monitoring</u></b>	Wahlverwalter	Kann alle Informationen einsehen und Geschäfte des eigenen Mandanten kontrollieren, zurückweisen und freigeben.
21)	Zugriff auf ZH VOTING Ausmittlung Monitoring ist nur für Personen nötig, die Geschäfte sperren.	Wahlunterstützer	Kann alle Informationen einsehen und Geschäfte des eigenen Mandanten kontrollieren, zurückweisen und freigeben.
22)	<b><u>UAT ZH VOTING ...</u></b>	<b>Alle Applikationen der UAT ZH Umgebung sind für Gemeinden nicht relevant. Es dürfen den Gemeindeusern keine Berechtigungen für Applikationen mit dem Präfix UAT ZH VOTING erteilt werden.</b> Die für die Gemeinden relevanten Applikationen beginnen mit ZH VOTING!	