

Rollen und Berechtigungen

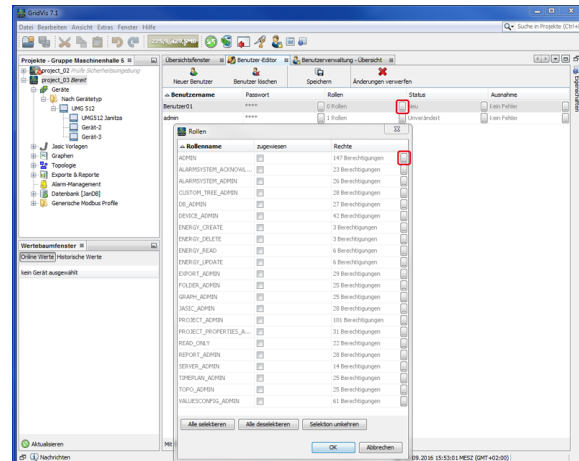
- In der **Benutzerverwaltung** der Software-GridVis vergeben Sie **Rollen** mit entsprechenden **Berechtigungen** an Benutzer.
- Benutzer** und **Rollen** (Gruppe von Berechtigungen) erstellen, vergeben und verwalten Sie im **Benutzer-Editor**.

HINWEIS!



- Die Funktion **Benutzerverwaltung** in der Software-GridVis ist in ständiger Bearbeitung. Damit einhergehend ändern sich auch **Rollen** und **Berechtigungen** der Benutzer. Die aktuellste Liste mit **Rollen** und **Berechtigungen** finden Sie in der **Benutzeroberfläche** Ihrer Software-GridVis.
- Die GridVis-Edition (Standard, Expert) mit der Webvisualisierungssoftware GridVis-Energy erlaubt **Benutzerverzeichnisse** und deren **Rollen** (**Berechtigungen**) direkt über die Weboberfläche zu konfigurieren und zu organisieren.
- Import- und Export-Funktionen in der **Benutzerverwaltung** Ihrer Software-GridVis-Desktop erlauben den Austausch von **Benutzerverzeichnissen** zwischen der Weboberfläche der GridVis-Energy und Ihrer GridVis-Desktop-Edition.
- In unten stehender Tabelle finden Sie ebenfalls **Rollen** (**Berechtigungen**), die auf die GridVis-Energy abgestimmt und zur **Benutzerverwaltung** (GridVis-Desktop) hinzugefügt wurden.

Abb.: Fenster "Rollen" im Benutzer-Editor



Um eine ausführliche Liste der Rollen (Fenster **Rollen** in der Software-GridVis) mit Ihren **Berechtigungen** zu sehen, gehen Sie als **Benutzer** mit eingeschränkten **Berechtigungen** wie folgt vor:

- Nachdem Sie der GridVis-Administrator als Benutzer angelegt hat, melden Sie sich mit Ihrem **Benutzernamen** und **Passwort** an Ihrem GridVis-Projekt an (Fenster **Benutzerverwaltung-Übersicht** --> unter Benutzer-Aktionen **Anmelden**).
- Nach erfolgreicher Anmeldung klicken Sie im Fenster **Benutzer-Editor** unter dem Eintrag **Rollen** auf die Schaltfläche "...".
- Es erscheint das Fenster **Rollen**.
- Um die **Berechtigungen** der einzelnen **Rollen** zu sehen, klicken Sie auf die Schaltfläche "...". in der entsprechenden **Rollen-Zeile** (siehe Abb. rechts).
- Es erscheint das Fenster **Berechtigungen**.

Die folgende Tabelle zeigt auszugsweise **Rollen** mit den wichtigsten **Berechtigungen**:

	Rollen	Auszug aus den wichtigsten Berechtigungen der Rollen
1	ADMIN	Administrator der Software GridVis. Der Benutzer mit der Rolle Administrator besitzt erweiterte Berechtigungen, u.a. für: <ul style="list-style-type: none"> Benutzer anlegen / ändern / löschen, Datenbank anlegen / verwalten / optimieren, Projekte anlegen / ändern / löschen, Geräte hinzufügen / ändern / löschen, Topologien hinzufügen / ändern / löschen, Graphen hinzufügen / ändern / löschen, Jasic-Dateien anlegen / ändern / verwalten, Reports hinzufügen / ändern / löschen, Werte löschen, Zeitpläne erstellen / löschen / verwalten.
2	ALARMSYSTEM_ACKNOWLEDGER	Benutzer mit der Rolle Administrator zur Bestätigung des Alarmsystems. Besitzt neben den Grundrechten READ_ONLY u.a. die Berechtigungen: <ul style="list-style-type: none"> Aktualisieren eines Elements im Alarmsystem. Lesen eines Elements im Alarmsystem.

3	ALARMSYSTEM_ADMIN	Benutzer mit der Rolle Administrator für das Alarmsystem . Besitzt neben den Grundrechten READ_ONLY u.a. die Berechtigungen: <ul style="list-style-type: none"> • Aktualisieren eines Elements im Alarmsystem. • Lesen eines Elements im Alarmsystem. • Erstellen und Löschen von Elementen im Alarmsystem.
4	CUSTOM_TREE_ADMIN	Benutzer mit der Rolle Administrator für eine benutzerdefinierte Baumstruktur . Besitzt neben den Grundrechten READ_ONLY die Berechtigungen: <ul style="list-style-type: none"> • benutzerdefinierte Bäume zu erstellen, zu löschen und zu editieren. • Verzeichnisse in benutzerdefinierten Bäume zu erstellen, zu löschen und zu sortieren.
5	DB_ADMIN	Benutzer mit der Rolle Administrator für den Bereich Datenbank . Besitzt neben den Grundrechten READ_ONLY die Berechtigung Datenbanken zu konfigurieren und zu verwalten.
6	DEVICE_ADMIN	Benutzer mit der Rolle Administrator für den Bereich Geräte . Besitzt neben den Grundrechten READ_ONLY die Berechtigungen: <ul style="list-style-type: none"> • Geräte anzulegen, zu löschen und zu konfigurieren, • Werte im Gerätespeicher zu löschen, • Zeitpläne für Gerätesynchronisation zu ändern / zu löschen, • Gerätefirmware zu aktualisieren, • Apps auf dem Gerät zu installieren.
7	ENERGY_CREATE	Benutzer mit der Rolle ENERGY_CREATE besitzt die Berechtigungen: <ul style="list-style-type: none"> • Bilder, Dashboards und Templates zu erstellen.
8	ENERGY_DELETE	Benutzer mit der Rolle ENERGY_DELETE besitzt die Berechtigungen: <ul style="list-style-type: none"> • Bilder, Dashboards und Templates zu löschen.
9	ENERGY_READ	Benutzer mit der Rolle ENERGY_READ besitzt die Berechtigungen: <ul style="list-style-type: none"> • Bilder, Dashboards, Dashboards-Favoriten und Templates zu betrachten. • Geräte und Geräte-Templates zu betrachten.
10	ENERGY_UPDATE	Benutzer mit der Rolle ENERGY_UPDATE besitzt die Berechtigungen: <ul style="list-style-type: none"> • Bilder, Dashboards, Dashboards-Favoriten und Templates zu bearbeiten. • Geräte zu editieren. • Template-Zuweisungen ändern.
11	EXPORT_ADMIN	Benutzer mit der Rolle Administrator für den Bereich Export . Besitzt neben den Grundrechten READ_ONLY u.a. die Berechtigungen: <ul style="list-style-type: none"> • Datenexporte zu aktualisieren, speichern, löschen und lesen. • Export-Zeitpläne zu erstellen, ändern, lesen, löschen und speichern.
12	FOLDER_ADMIN	Benutzer mit der Rolle Administrator für den Bereich Verzeichnisse . Besitzt neben den Grundrechten READ_ONLY u.a. die Berechtigungen: <ul style="list-style-type: none"> • Ordnerverzeichnisse zu erstellen, aktualisieren, bearbeiten, löschen und lesen.
13	GRAPH_ADMIN	Benutzer mit der Rolle Administrator für den Bereich Graphen . Besitzt neben den Grundrechten READ_ONLY die Berechtigungen: <ul style="list-style-type: none"> • Graphen anzulegen, zu löschen und zu verwalten.
14	JASIC_ADMIN	Benutzer mit der Rolle Administrator für den Bereich Jasic . Besitzt neben den Grundrechten READ_ONLY die Berechtigungen: <ul style="list-style-type: none"> • Jasic-Dateien anzulegen, zu löschen und zu verwalten.

15	PROJECT_ADMIN	Benutzer mit der Rolle Administrator für das Projekt. Besitzt die gleichen Berechtigungen wie der Administrator , kann aber keine Benutzer anlegen und verwalten.
16	PROJECT_PROPERTIES_ADMIN	Benutzer mit der Rolle Administrator für Projekteigenschaften. Besitzt neben den Grundrechten READ_ONLY die Berechtigung Projekt-Eigenschaften zu aktivieren und zu verwalten.
17	READ_ONLY	Benutzer mit Grundrechten zum Lesen
18	REPORT_ADMIN	Benutzer mit der Rolle Administrator für den Bereich Reports. Besitzt neben den Grundrechten READ_ONLY die Berechtigungen: <ul style="list-style-type: none"> • Reports anzulegen, zu löschen und zu verwalten.
19	SERVER_ADMIN	Benutzer mit der Rolle Administrator für den Bereich Server. Besitzt neben den Grundrechten READ_ONLY u.a. die Berechtigungen: <ul style="list-style-type: none"> • Bilder, Dashboards, Dashboards-Favoriten und Templates zu betrachten. • Geräte und Geräte-Templates zu betrachten. • Systemeinstellungen für den Dienst zu lesen, bearbeiten, hinzufügen und löschen. • Benutzer zu betrachten, wechseln, anlegen und löschen.
20	TIMEPLAN_ADMIN	Benutzer mit der Rolle Administrator für Zeitpläne. Besitzt neben den Grundrechten READ_ONLY die Berechtigungen: <ul style="list-style-type: none"> • Zeitpläne zu erstellen, zu löschen und zu editieren.
21	TOPO_ADMIN	Benutzer mit der Rolle Administrator für den Bereich Topologie. Besitzt neben den Grundrechten READ_ONLY die Berechtigungen: <ul style="list-style-type: none"> • Topologieseiten zu erstellen, zu löschen und zu editieren.
22	VALUESCONFIG_ADMIN	Benutzer mit der Rolle Administrator für den Bereich Wertekonfiguration. Besitzt neben den Grundrechten READ_ONLY u.a. die Berechtigungen: <ul style="list-style-type: none"> • Datenbanken zu konfigurieren, importieren, verwalten, migrieren und optimieren. • Datenbankaktionen zu lesen und aktualisieren. • Wertekonfigurationen lesen und ändern. • Reporte zu öffnen, ändern, auszuführen. • u.a.