

Administration

- [Anmeldung als SuperUser](#)
- [Rollen und Berechtigungen](#)
- [Benutzer und Rollen](#)
- [Dashboard Berechtigungen](#)
- [API zum Abrufen von Dashboards](#)
- [Lizenz beantragen](#)

Anmeldung als SuperUser

In der Konfigurationsdatei **appsettings.json** auf Serverebene gibt es im Bereich **Security** den Parameter **SuperUser**. Wird dieser auf den Wert **Active** gesetzt, so ist es möglich sich als SuperUser an RiskBoards anzumelden. Standardmäßig muß dieser Wert auf **Inactive** stehen.

Diesen Administrationsmodus nur verwenden wenn kein externer Zugriff auf das System möglich ist!

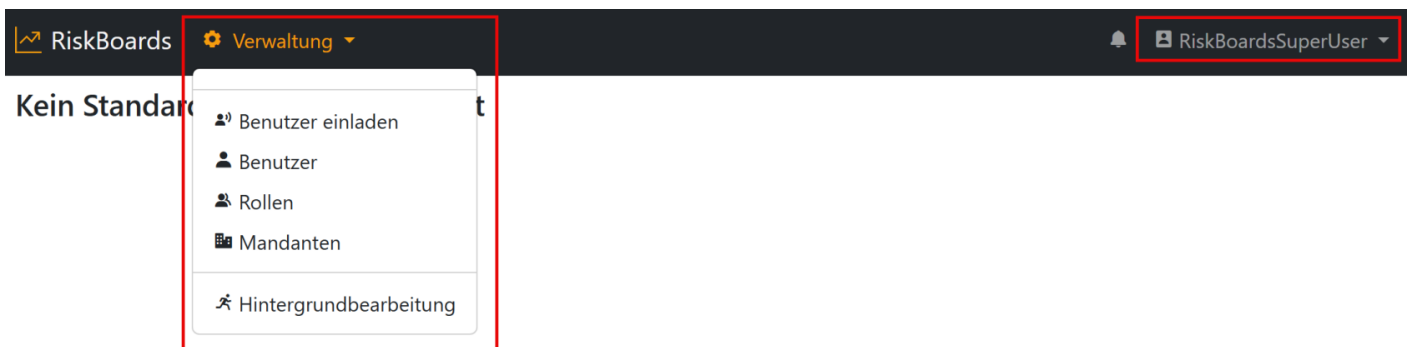
Diesen Administrationsmodus nach Nutzung umgehend wieder deaktivieren!

```
"Security": {  
  "SuperUser": "Active",  
  "Authentication": {  
    "Mode": "Integrated",  
    "Integrated": {  
      }  
    },  
  "Negotiation": {  
    "SuperAdmin": {  
      }  
    }  
  }  
}
```

Ist der Administrationsmodus kurzfristig aktiviert, so kann über die folgende URL auf RiskBoards zugegriffen werden:

<https://servername/security/loginassuperuser>

Nach Aufruf der URL befindet man sich direkt im Verwaltungsmodus und kann beliebig Benutzer, Rollen oder Mandanten bearbeiten.

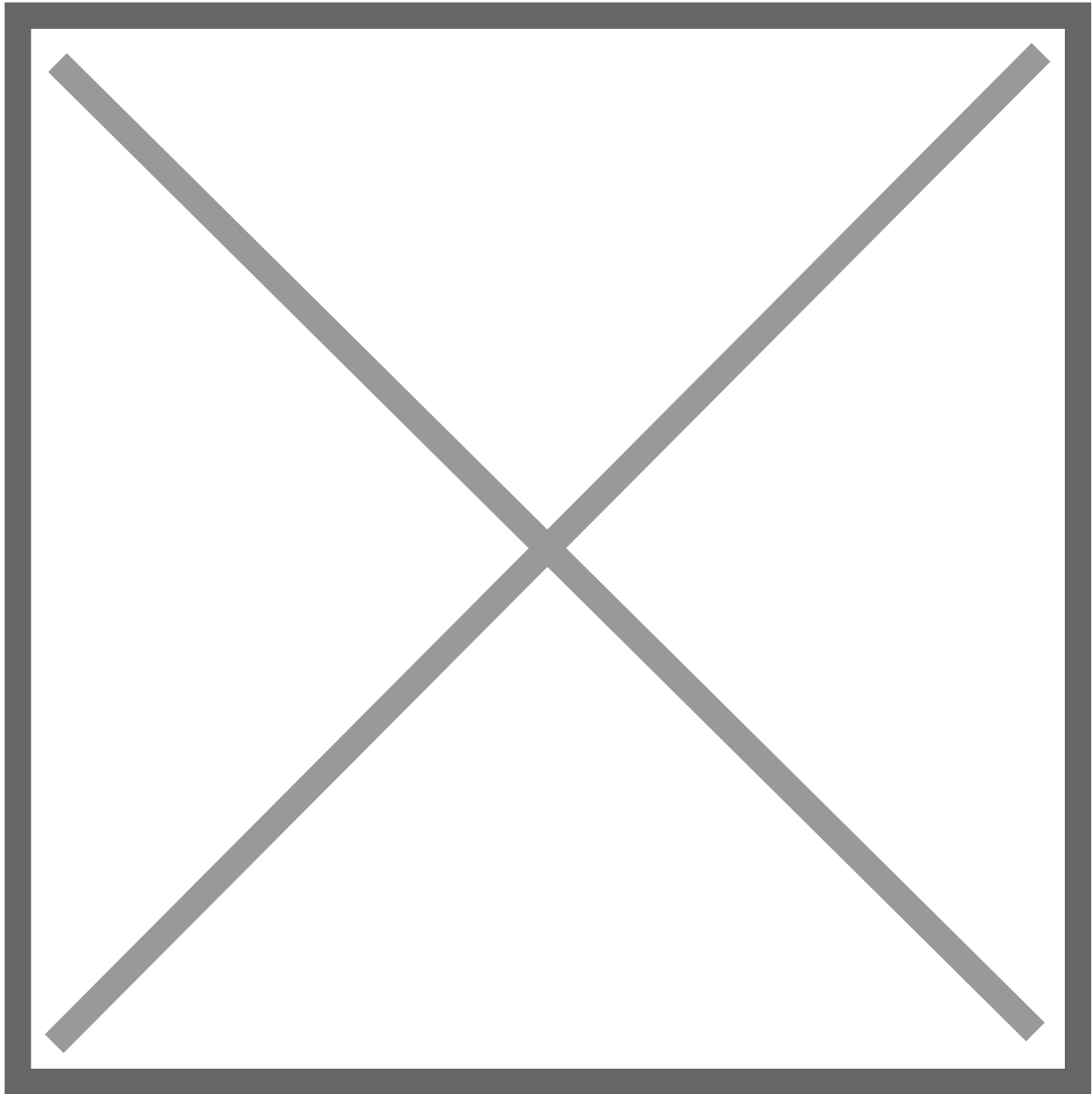


Dieser Modus ist im Speziellen dafür geeignet, noch auf das System zugreifen zu können, wenn aus unerfindlichen Gründen kein Administrator Benutzer mehr zur Verfügung steht.

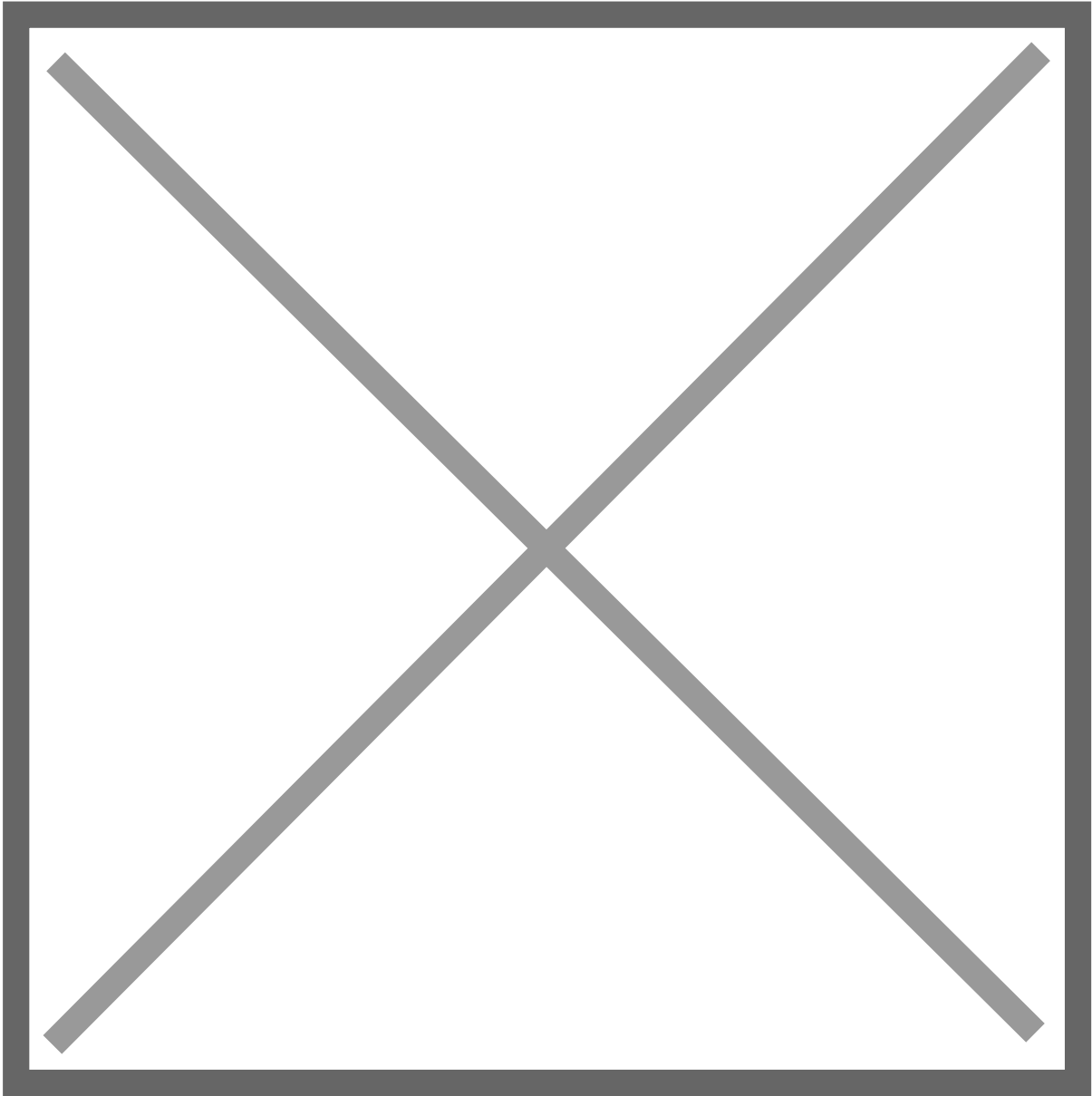
Rollen und Berechtigungen

RiskBoards bietet umfangreiche Berechtigungsmöglichkeiten die über Rollen gesteuert werden.

Rollen werden im Bereich Verwaltung erstellt und bearbeitet.

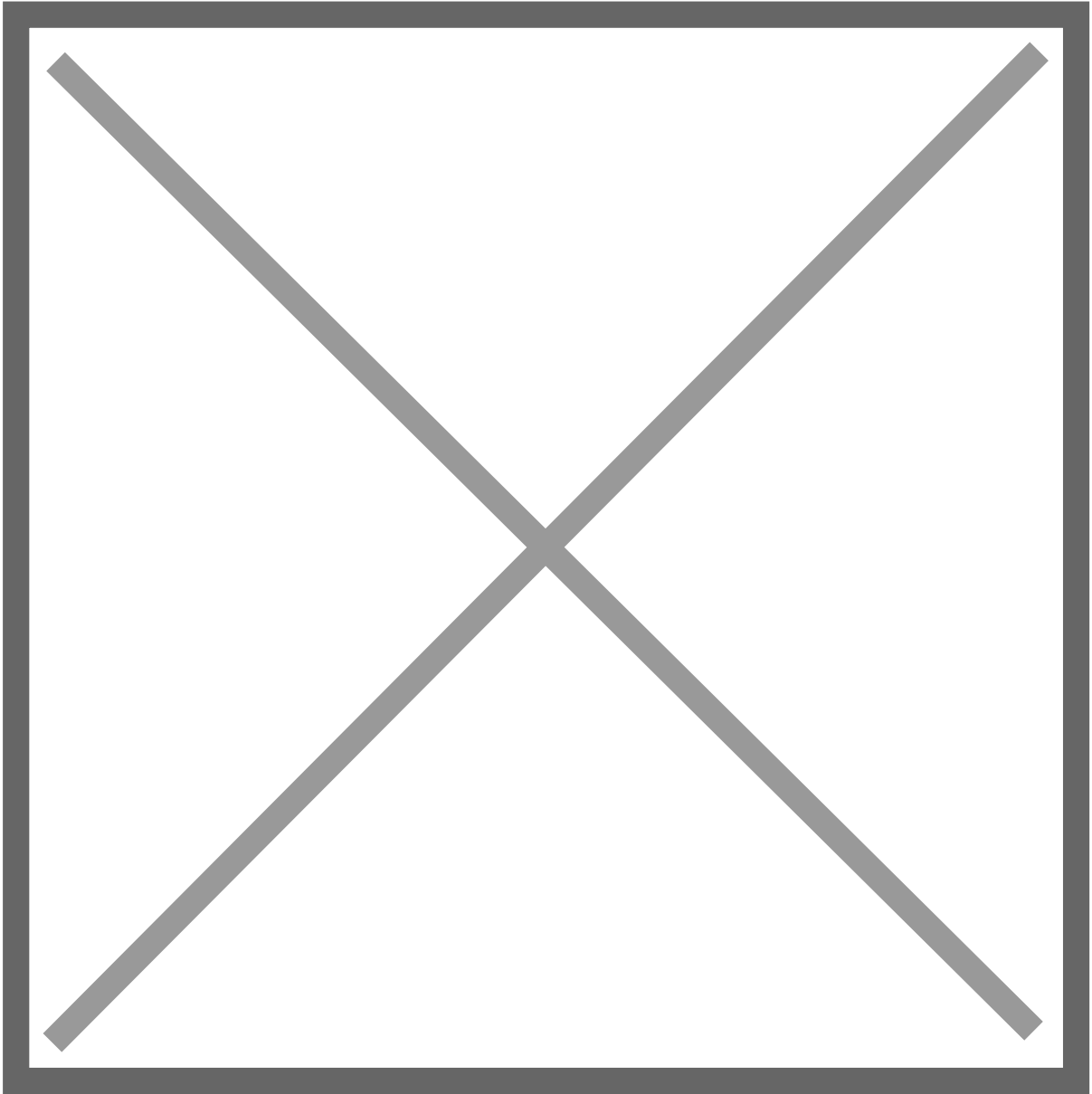


Das Anlegen einer neuen Rolle ist über das + im oberen rechten Bereich möglich.



Die Rolle muss einen eindeutigen Namen haben (im Beispiel „**Tenant DashboardAccessGroup1 User**“).

Sollen beispielsweise Dashboards für den Bereich Finanzen verwaltet werden, bietet sich z. B. **Finanzen** für den Namen der Rolle an. Im rechten Teil muss dieser Rolle die entsprechende Berechtigung oder mehrere Berechtigungen zugewiesen werden. Dies ist die Berechtigungsgruppe, welche im Dashboard über **Zugeordnete Gruppen** zugewiesen wird.

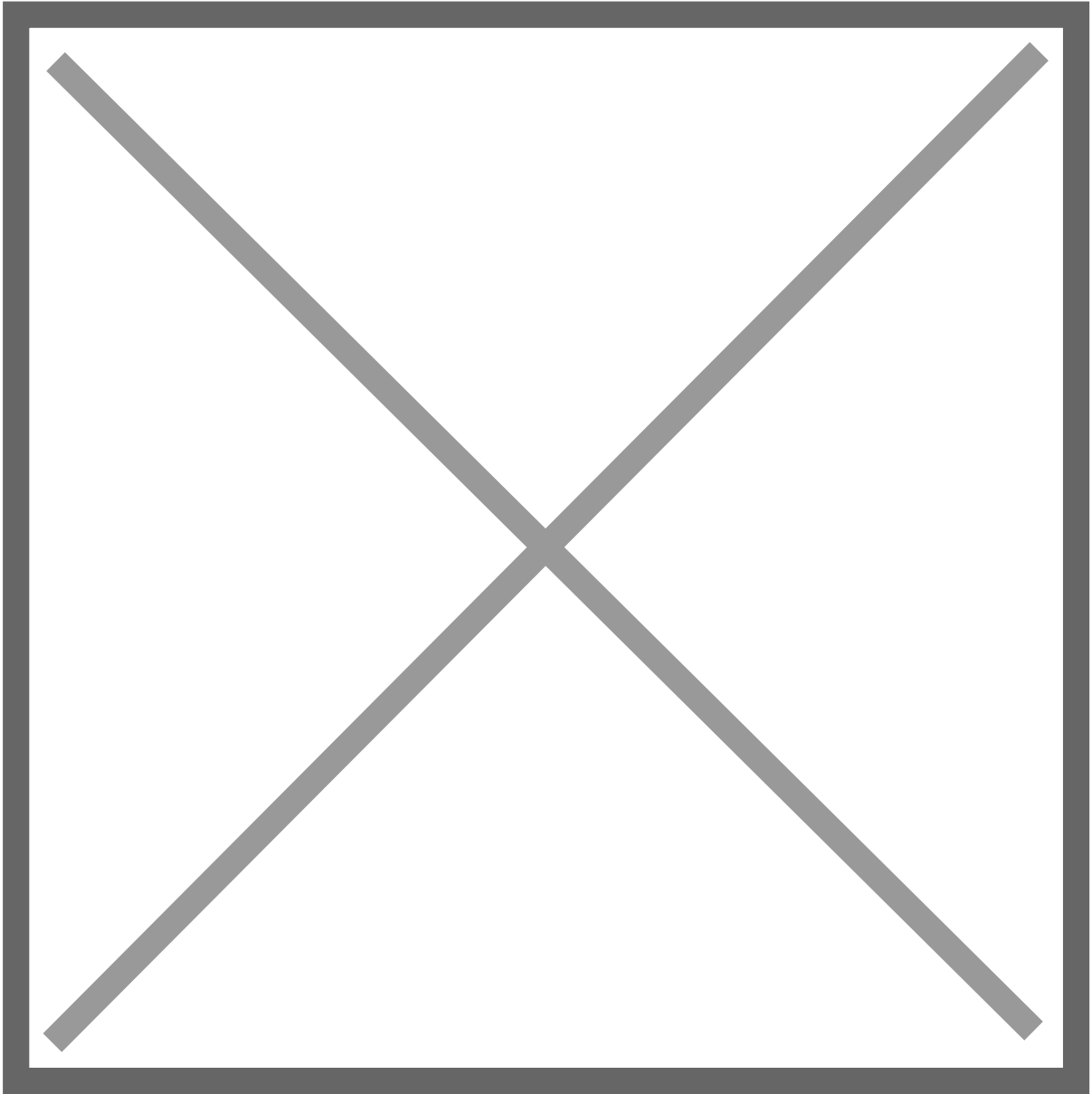


Einer Rolle können beliebige Berechtigungen zugewiesen werden.

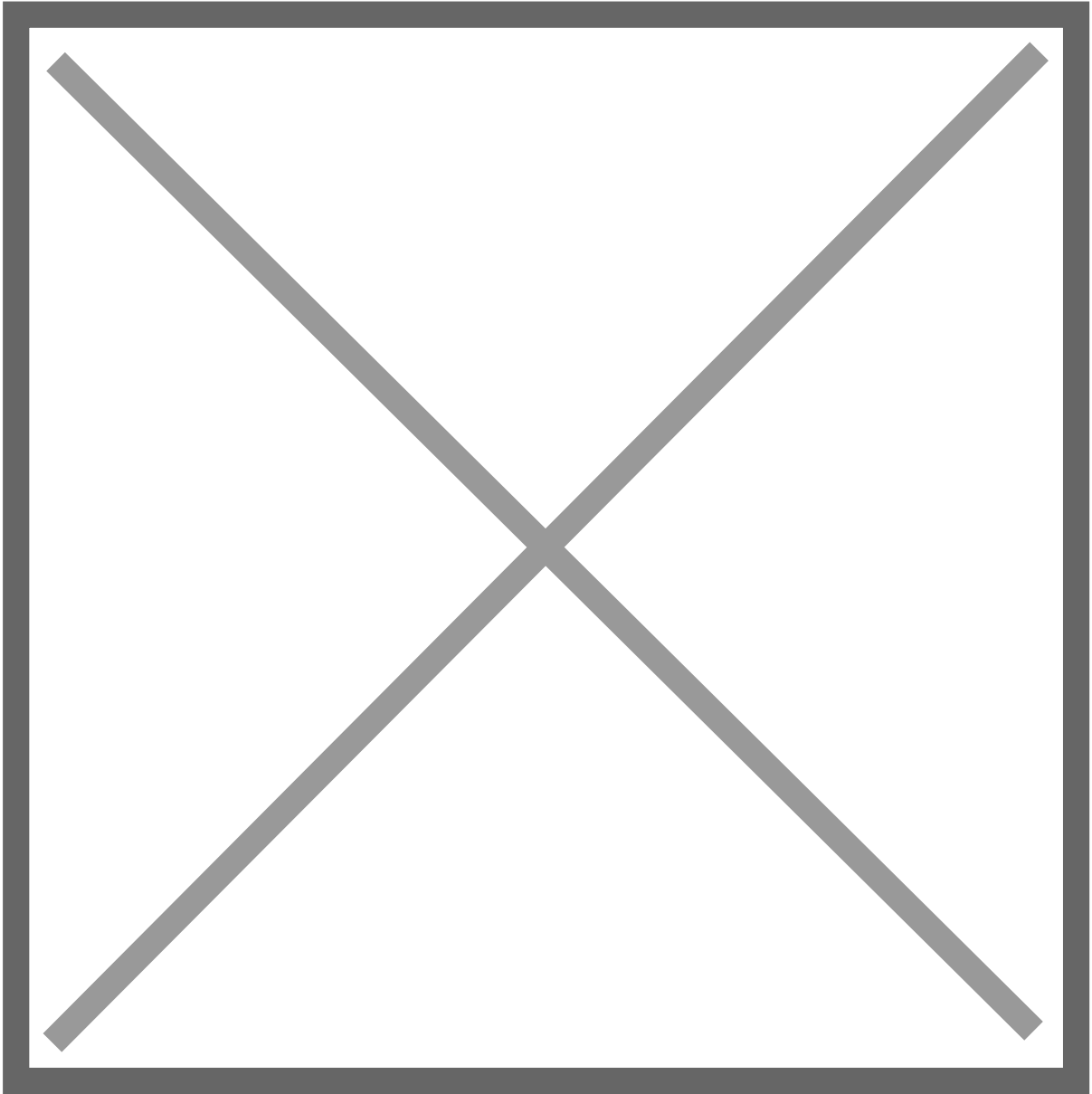
Mandanten

Um die Rolle im jeweiligen Mandanten verfügbar zu machen, ist diese im Mandanten als zulässige Rolle zu definieren.

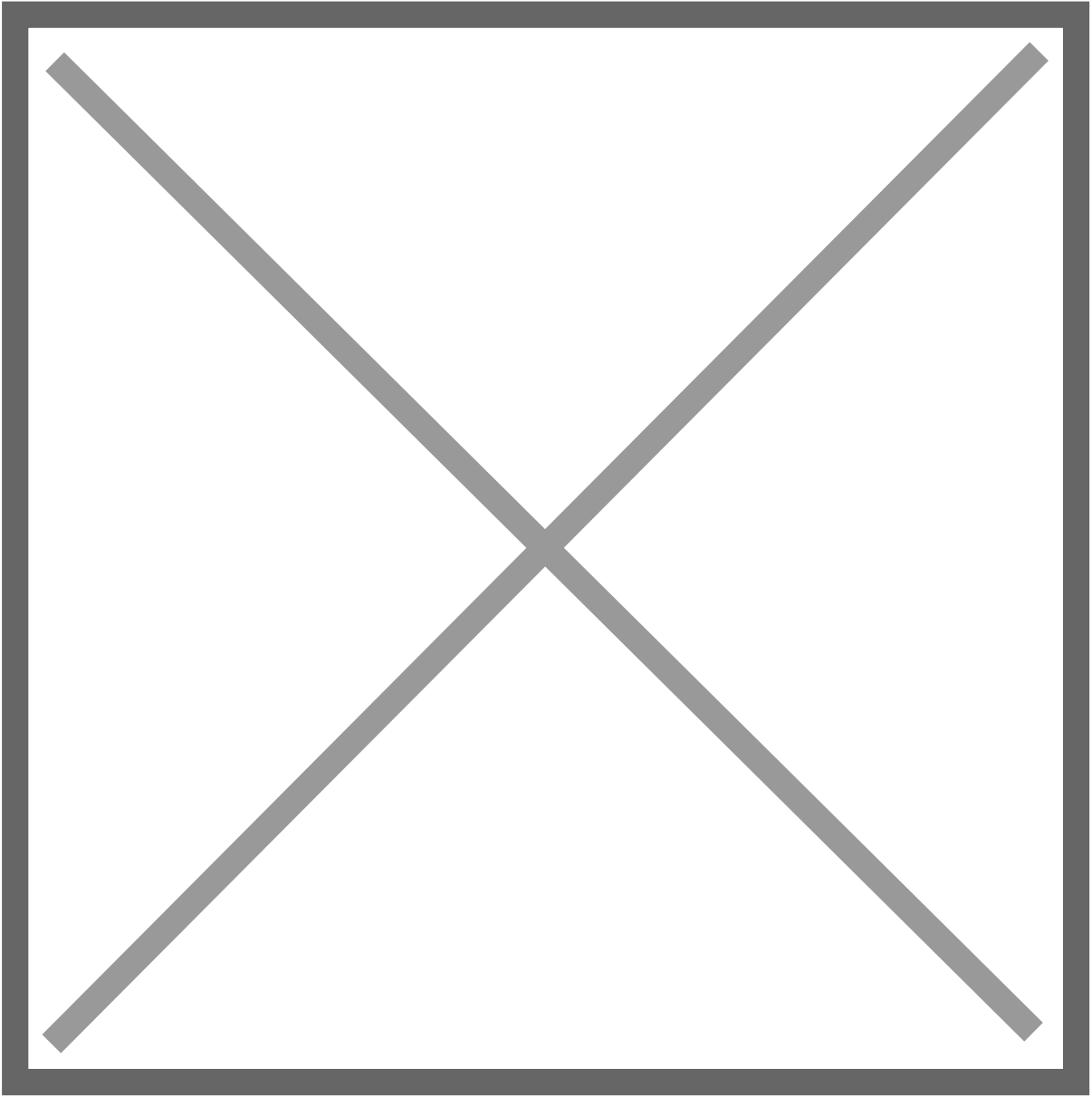
Mandanten werden im Bereich Verwaltung erstellt und bearbeitet.



Das Bearbeiten eines Mandanten erfolgt über das Stift Symbol im oberen rechten Bereich.

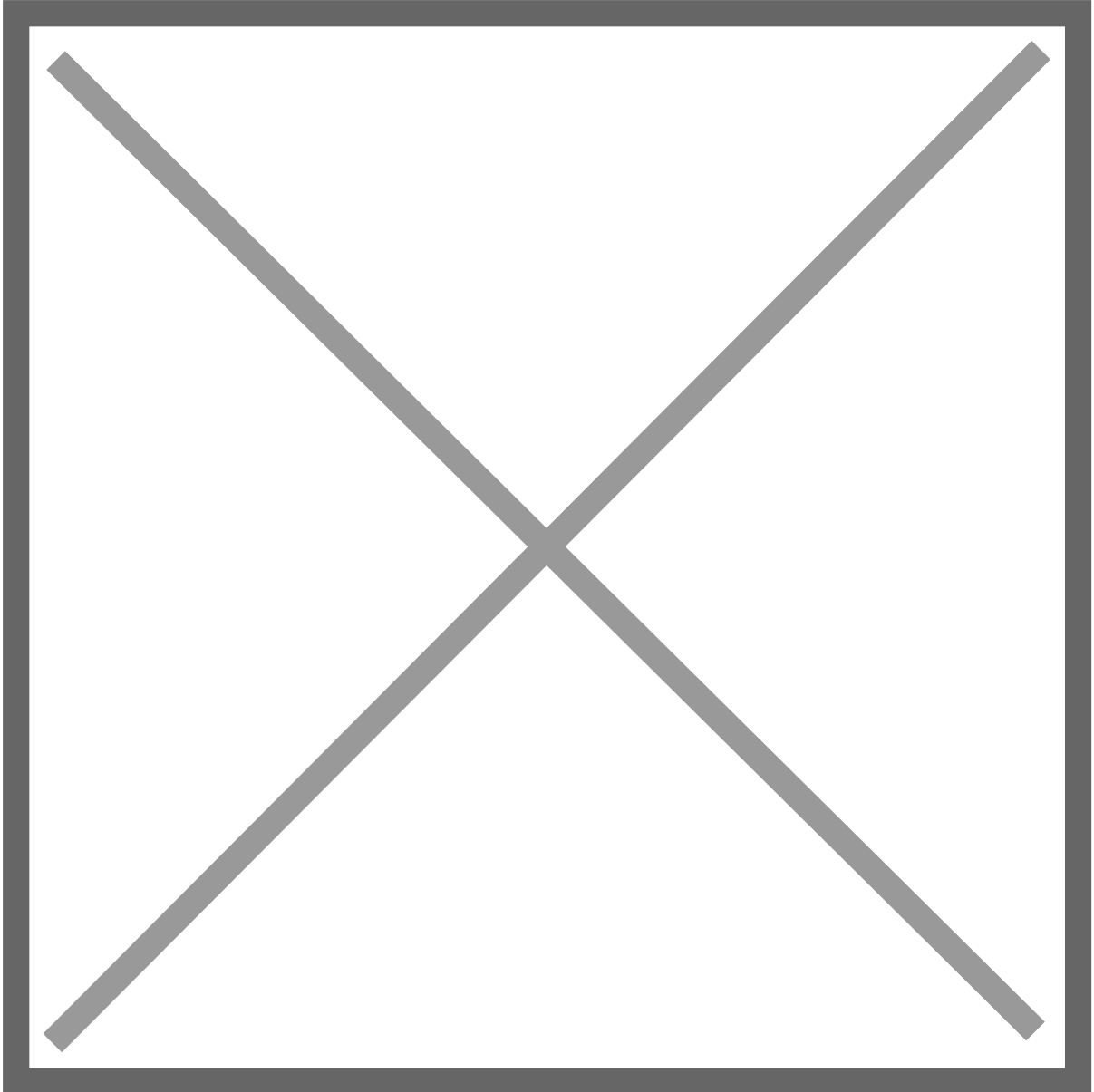


Im Bereich **Berechtigungen** sind die gewünschten Rollen dem Mandanten hinzuzufügen.

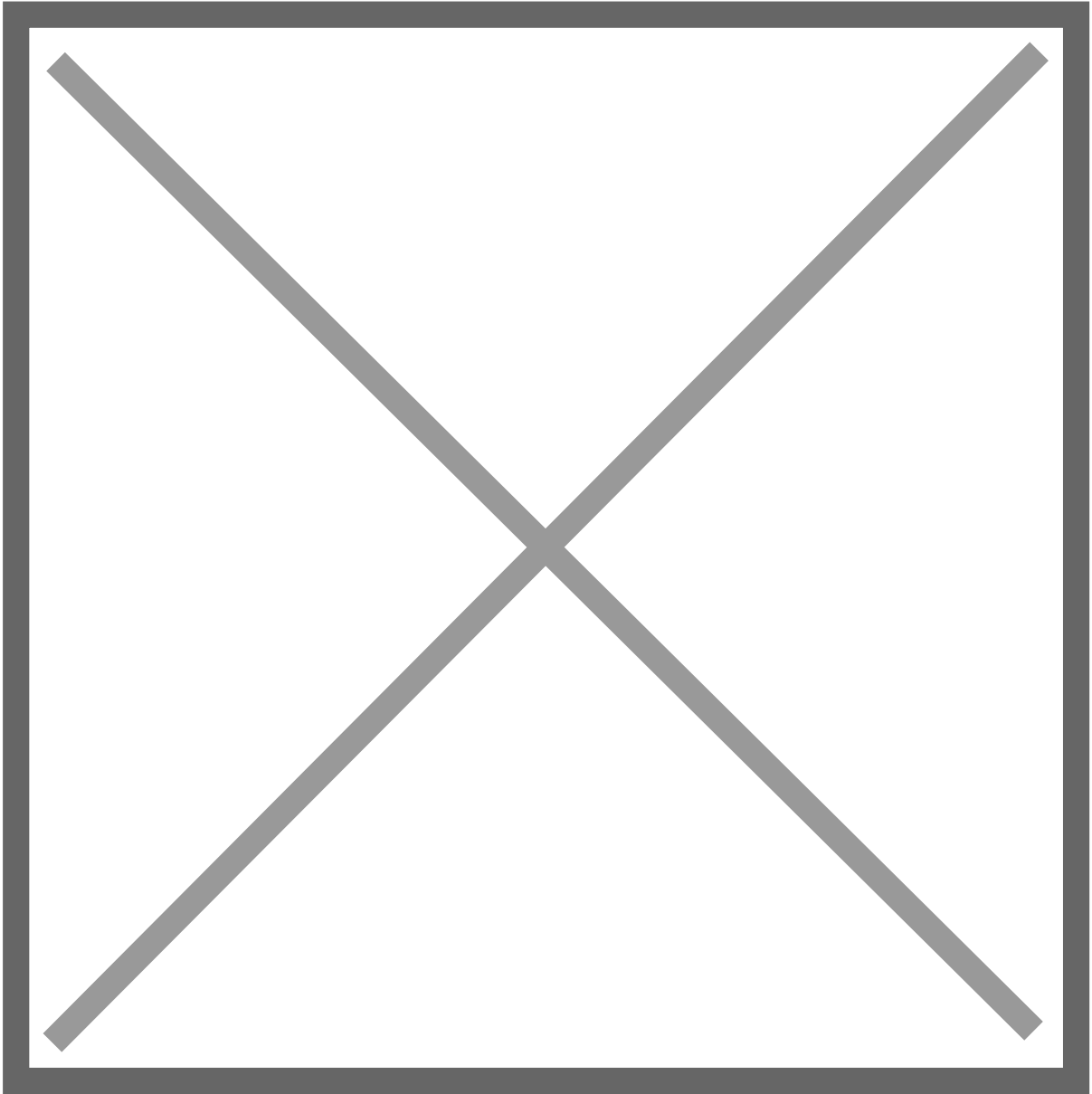


Benutzer und Rollen

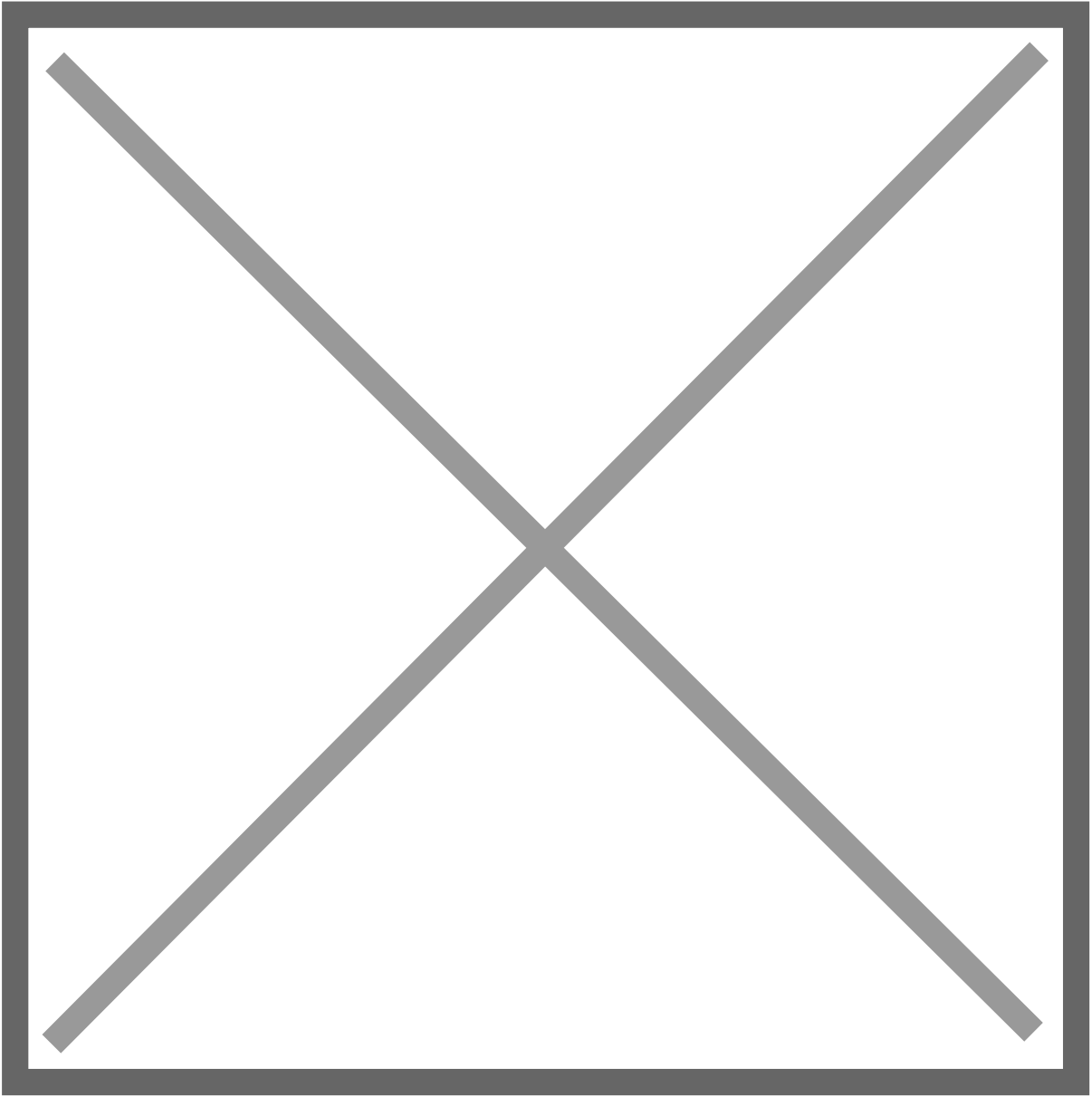
Um Benutzern Rollen zuzuweisen ist es notwendig, die definierten Rollen den gewünschten Benutzern zuzuordnen. Dies erfolgt über den Bereich Verwaltung.



Bearbeitet wird der gewünschte Benutzer über das Stift Symbol im rechten Bereich.



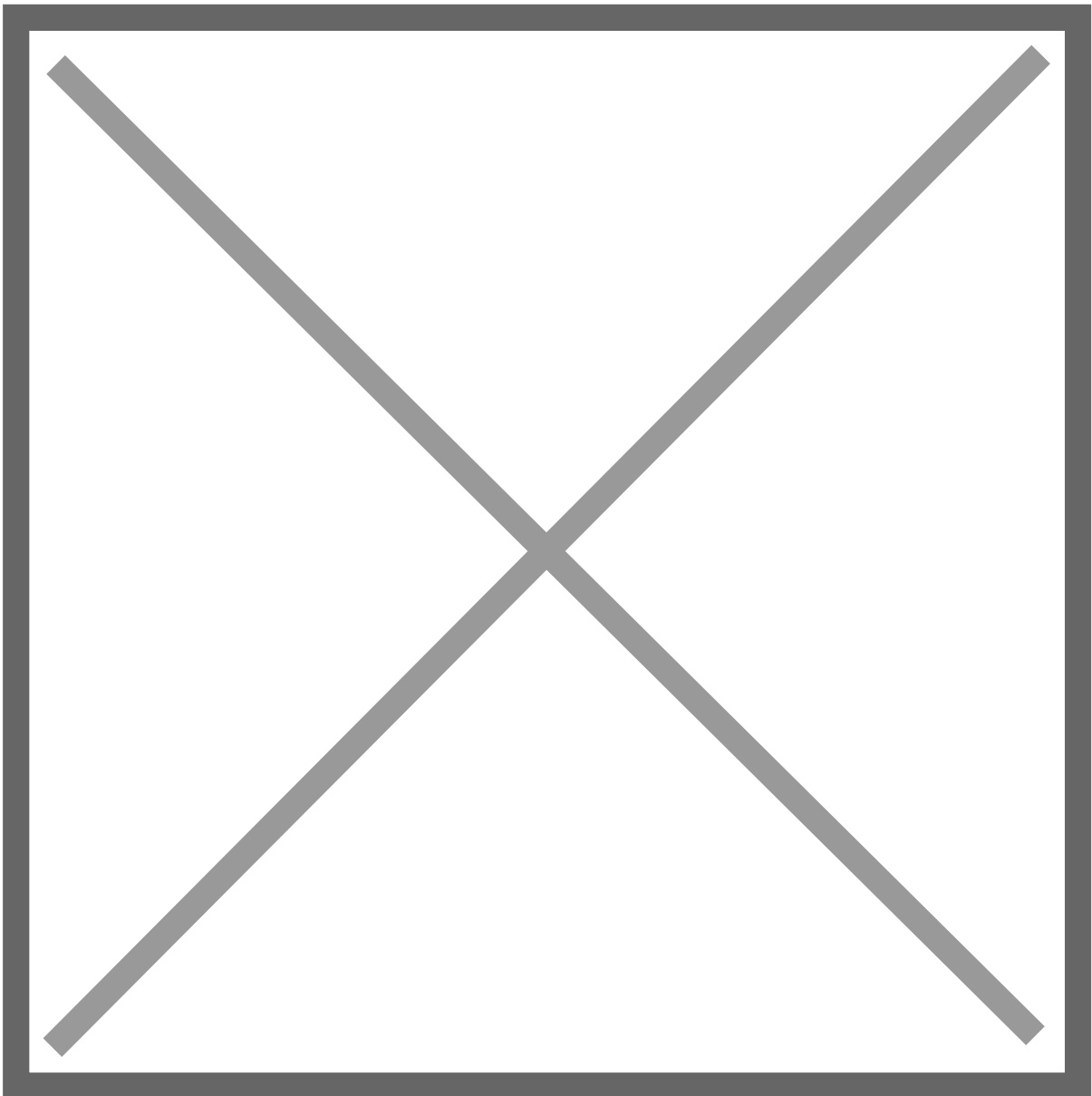
Im Bereich **Berechtigungen** ist bei **Rollen** die entsprechende Rolle oder auch mehrere auszuwählen.



Dashboard Berechtigungen

RiskBoards unterstützt die Möglichkeit Dashboards nur für bestimmte Benutzergruppen zugänglich zu machen, beispielsweise für Finanzcockpits, Unternehmenskennzahlen oder ähnliches.

Hierzu steht in den Metadaten eines Dashboards im Bereich **Berechtigungen** die Einstellung **Zugeordnete Gruppen** zur Verfügung. Es stehen 10 Gruppen zur Auswahl, welche beliebig in Dashboards verwendet werden können. Ein Dashboard kann auch mehreren Gruppen zugeordnet werden.

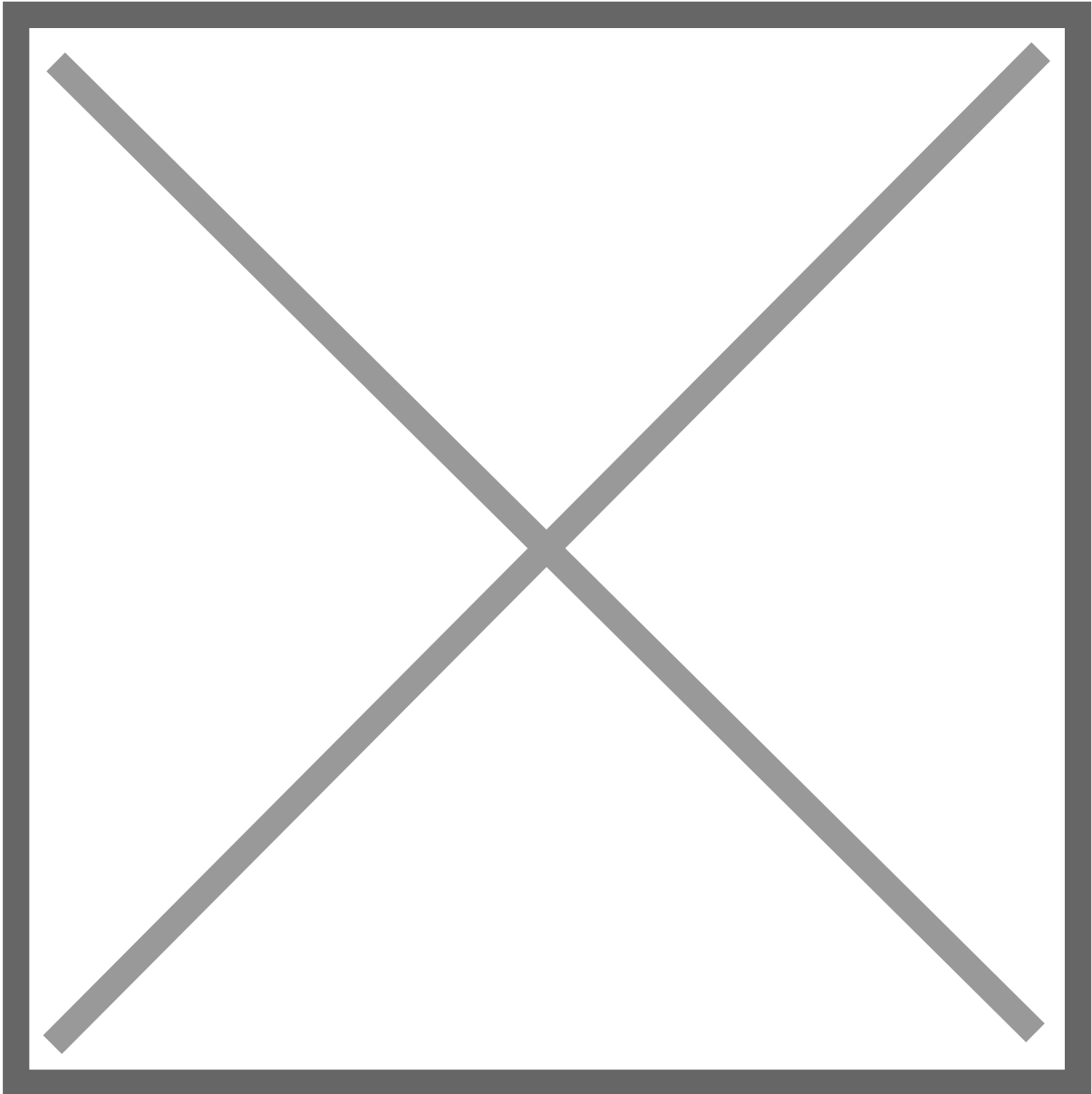


Administration

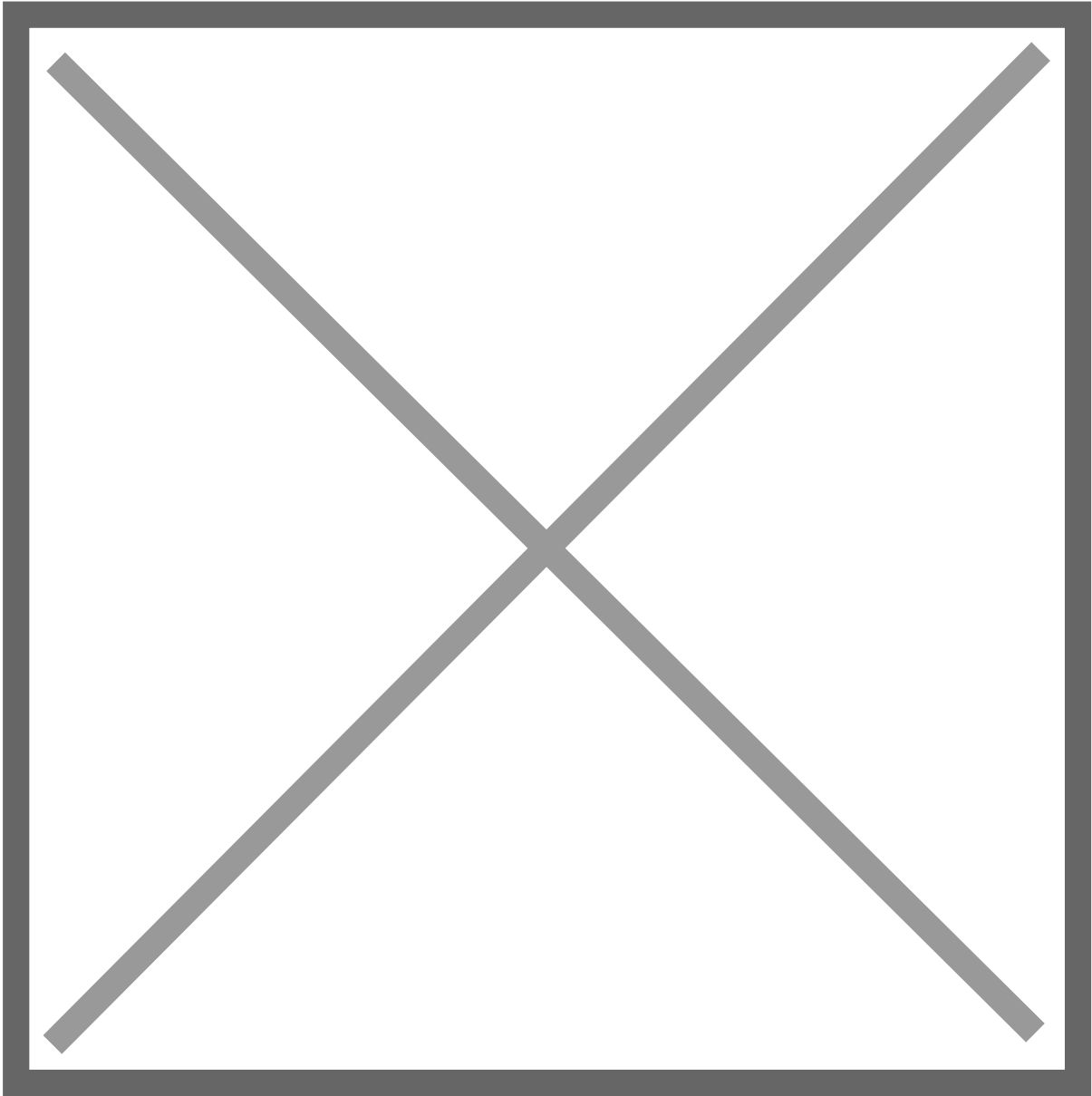
Rollen

Um die Funktionalität der Berechtigungen für Dashboards nutzen zu können, sind entsprechende Rollen zu definieren und den Benutzern zuzuweisen.

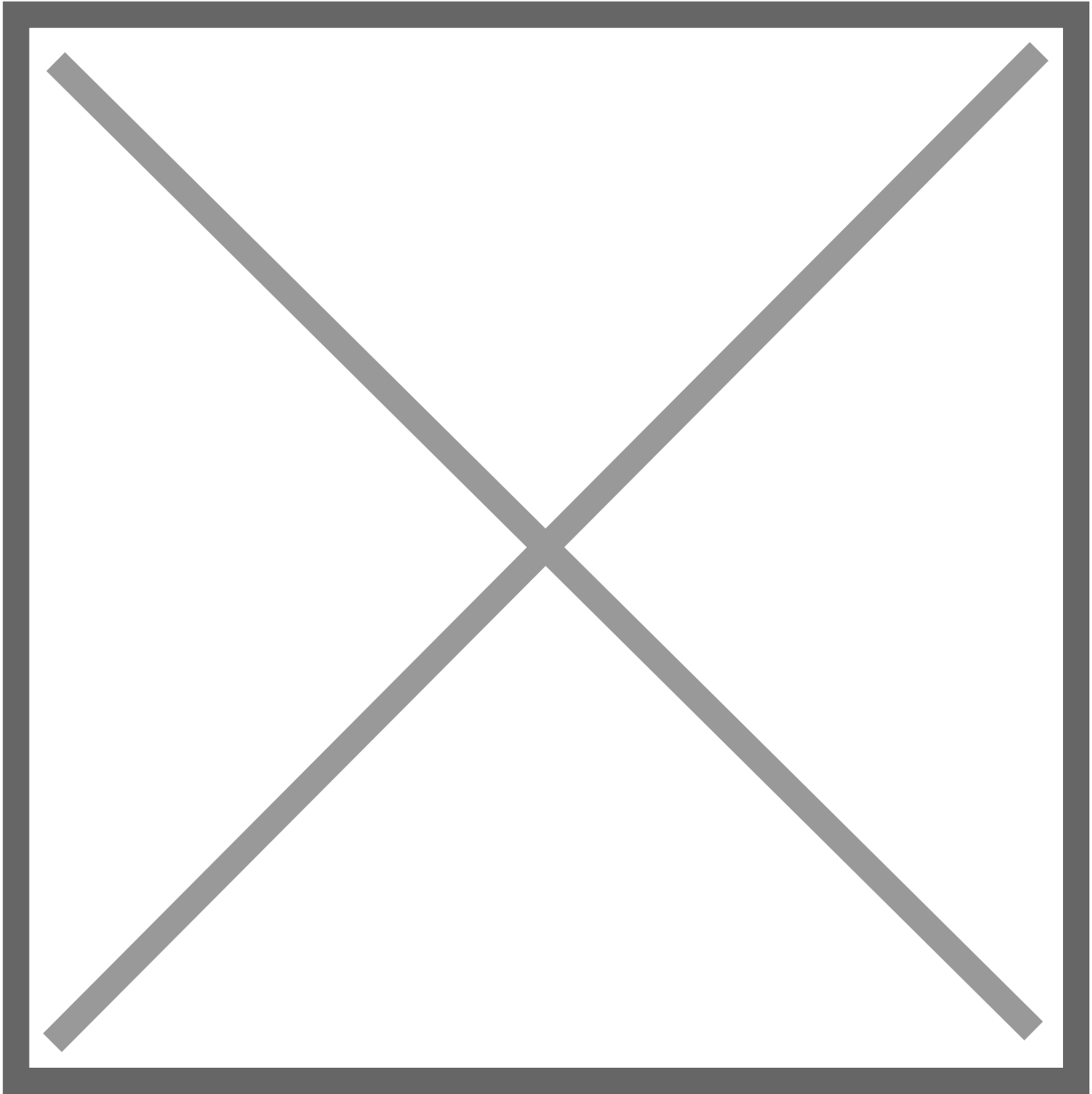
Rollen werden im Bereich Verwaltung erstellt und bearbeitet.



Das Anlegen einer neuen Rolle ist über das + im oberen rechten Bereich möglich.



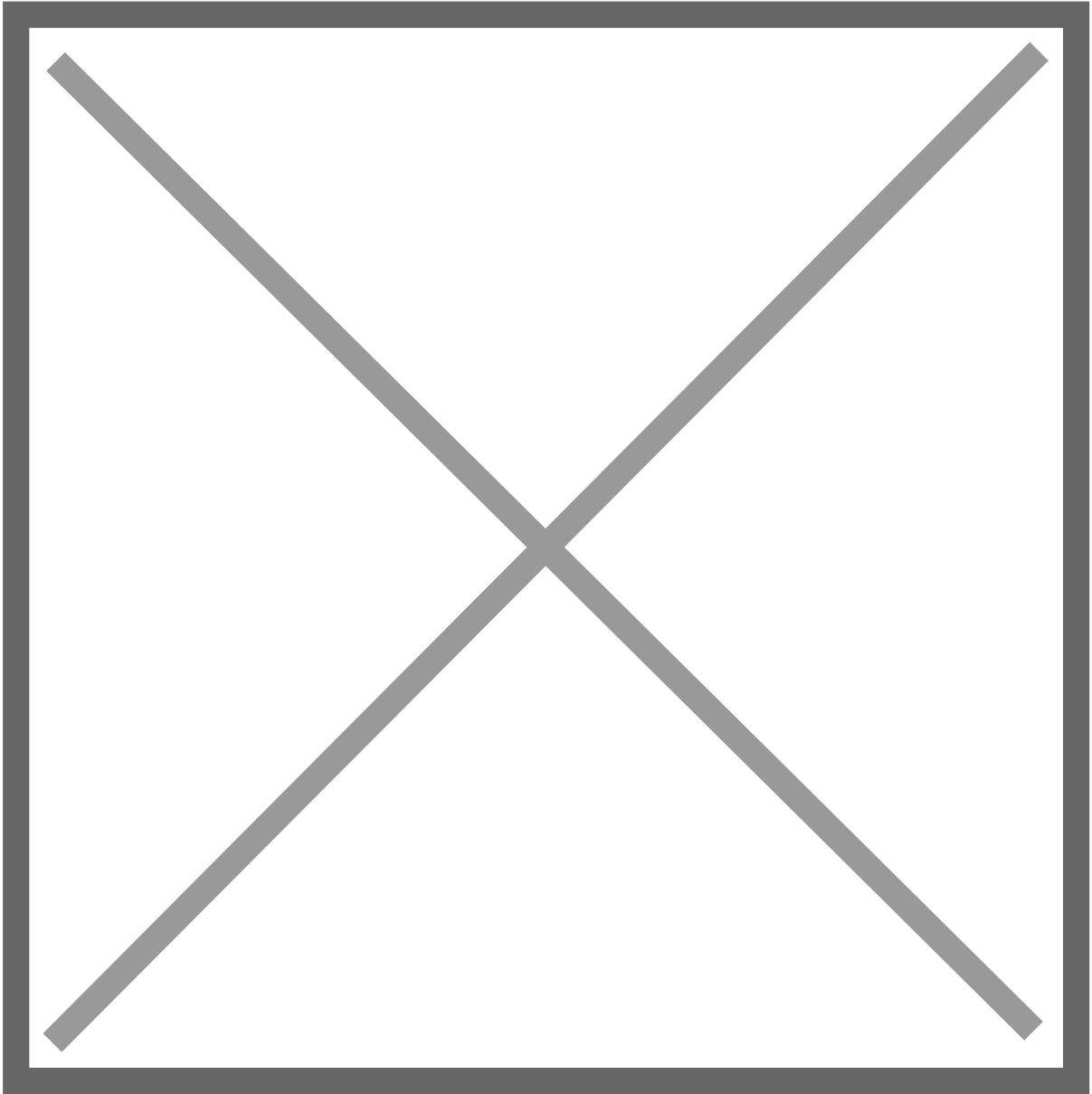
Die Rolle muss einen eindeutigen Namen haben (im Beispiel „**Tenant DashboardAccessGroup1 User**“). Sollen beispielsweise Dashboards für den Bereich Finanzen verwaltet werden, bietet sich z. B. **Finanzen** für den Namen der Rolle an. Im rechten Teil muss dieser Rolle die entsprechende Berechtigung oder mehrere Berechtigungen zugewiesen werden. Dies ist die Berechtigungsgruppe, welche im Dashboard über **Zugeordnete Gruppen** zugewiesen wird.



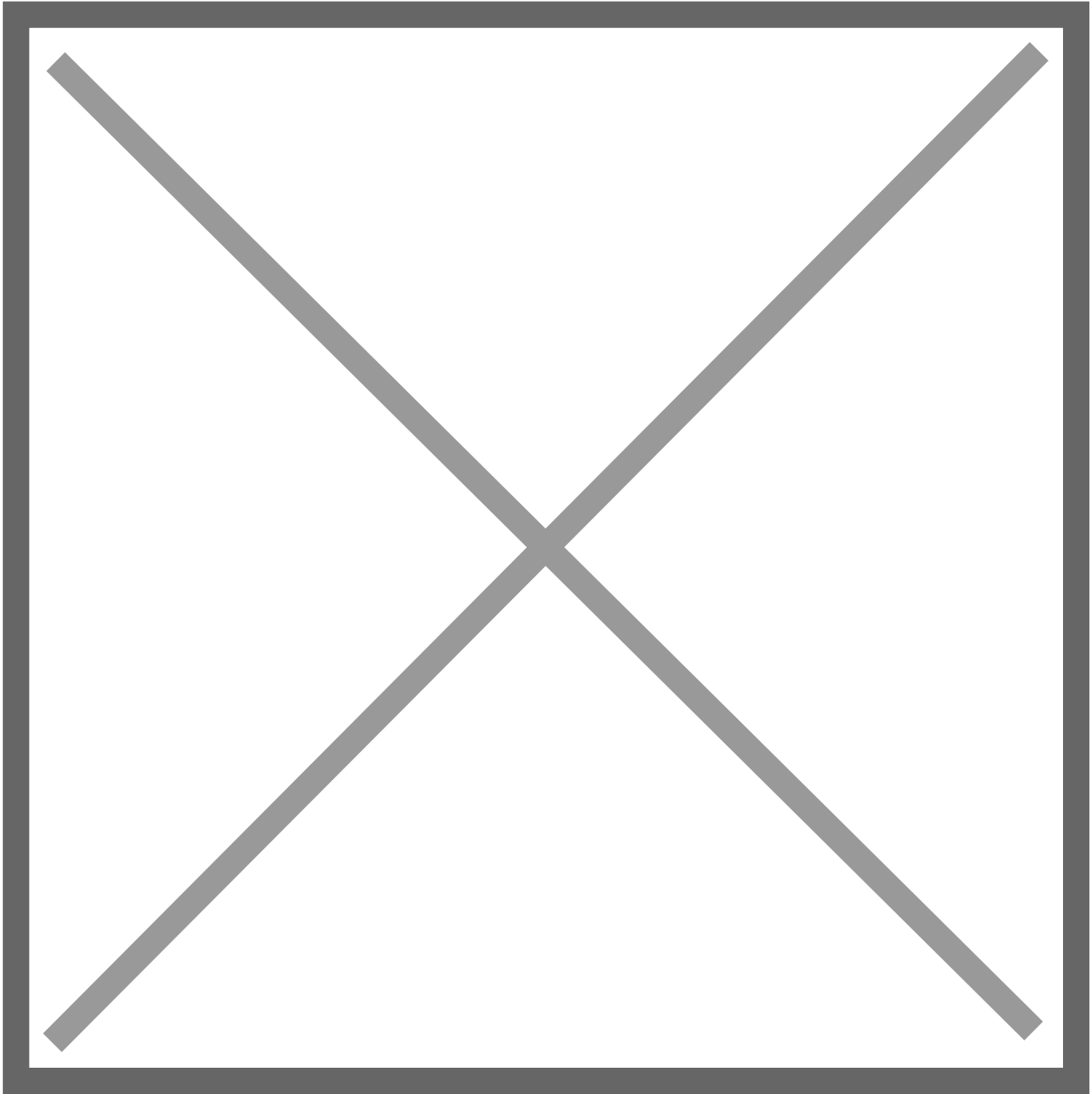
Mandanten

Um die Rolle im jeweiligen Mandanten verfügbar zu machen, ist diese im Mandanten als zulässige Rolle zu definieren.

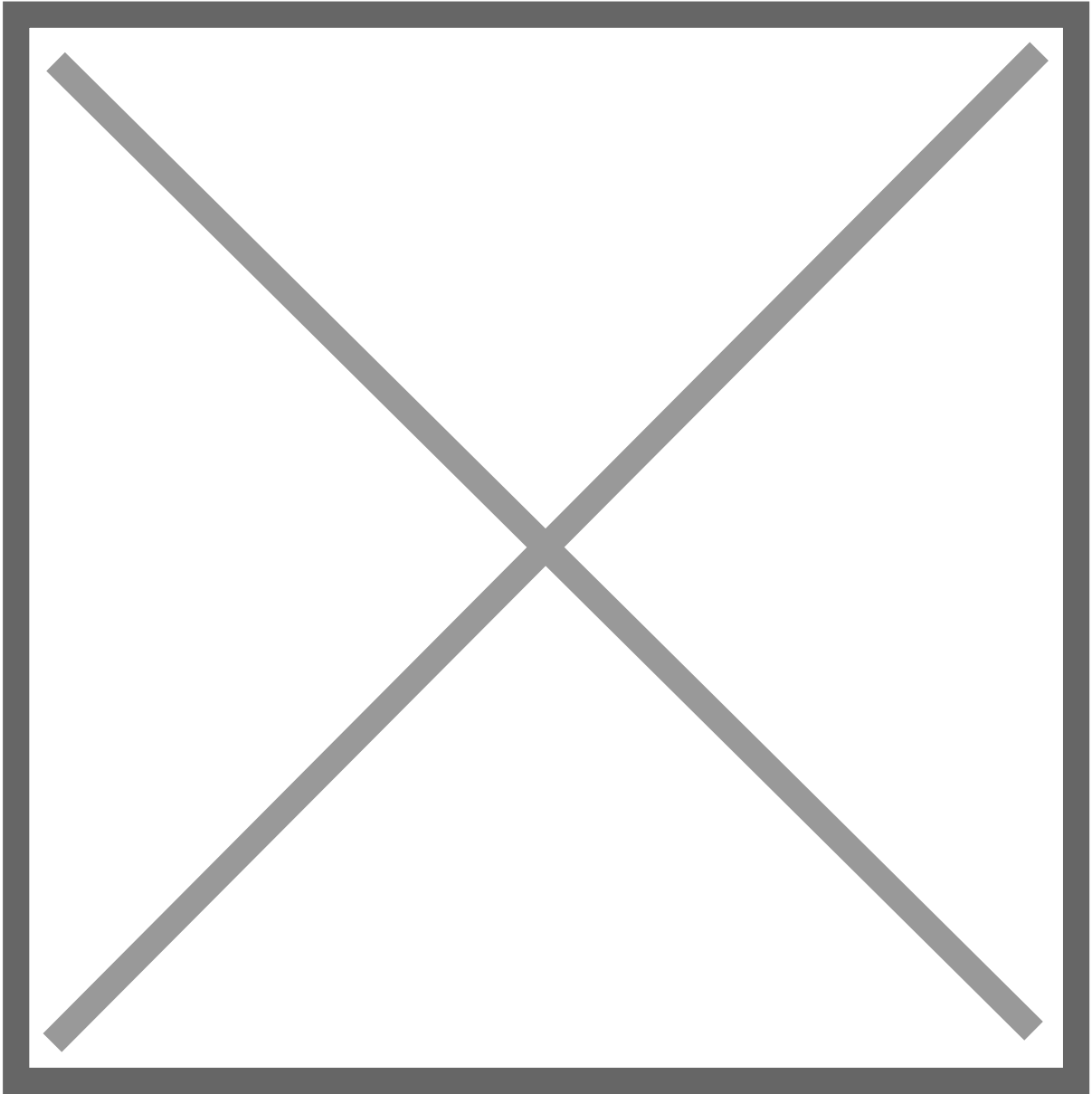
Mandanten werden im Bereich Verwaltung erstellt und bearbeitet.



Das Bearbeiten eines Mandanten erfolgt über das Stift Symbol im oberen rechten Bereich.

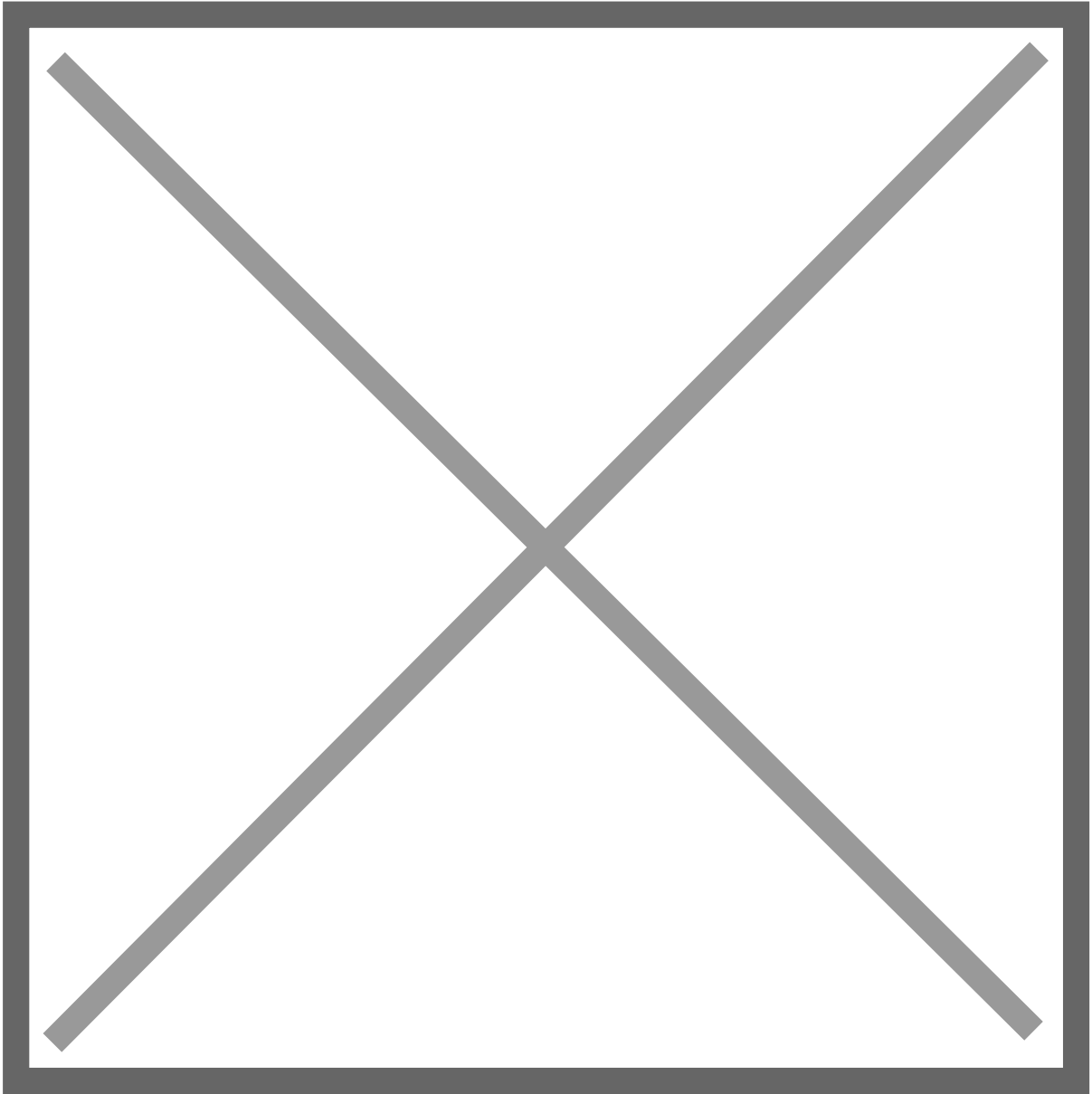


Im Bereich **Berechtigungen** sind die gewünschten Rollen dem Mandanten hinzuzufügen.

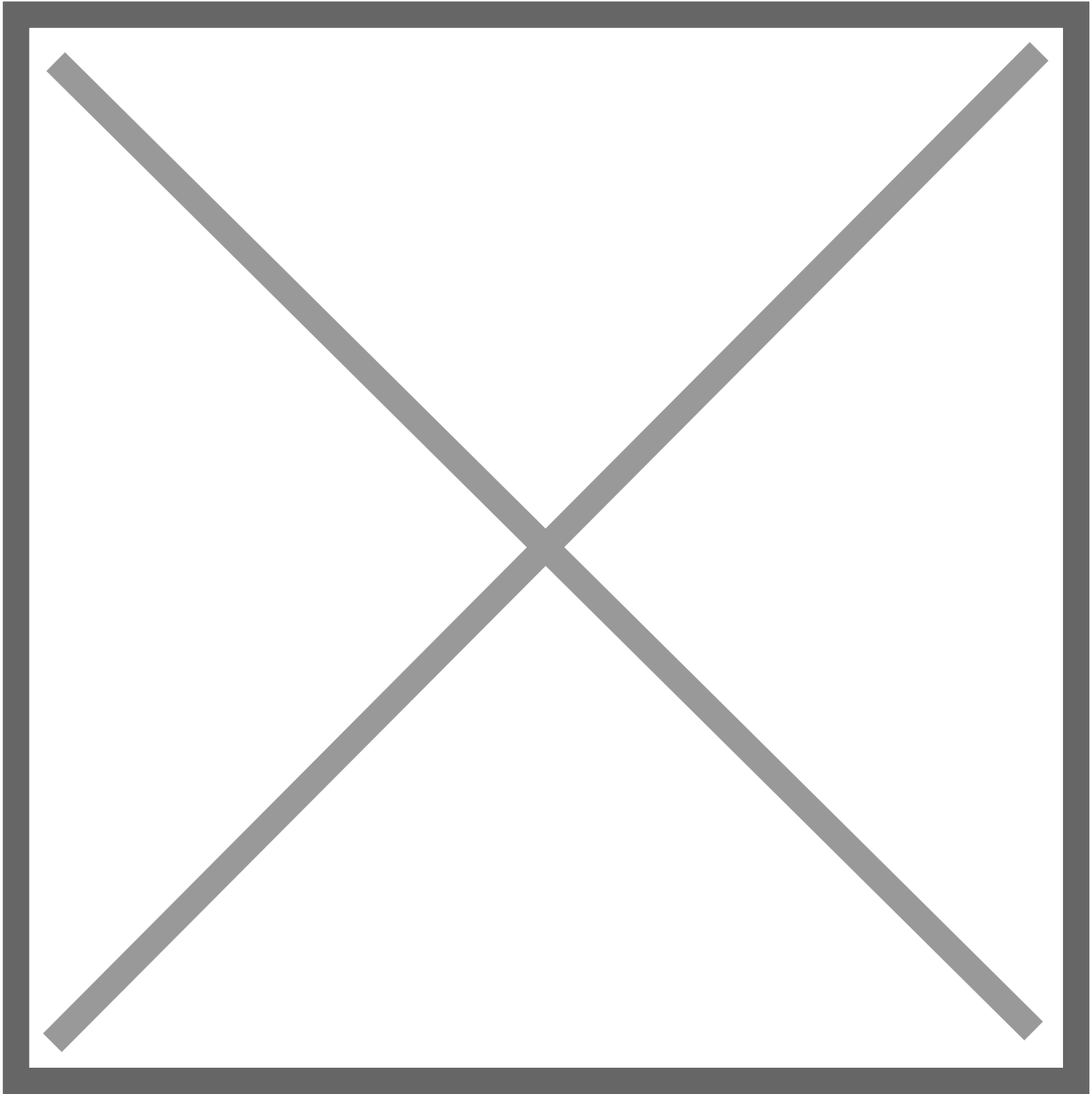


Benutzer

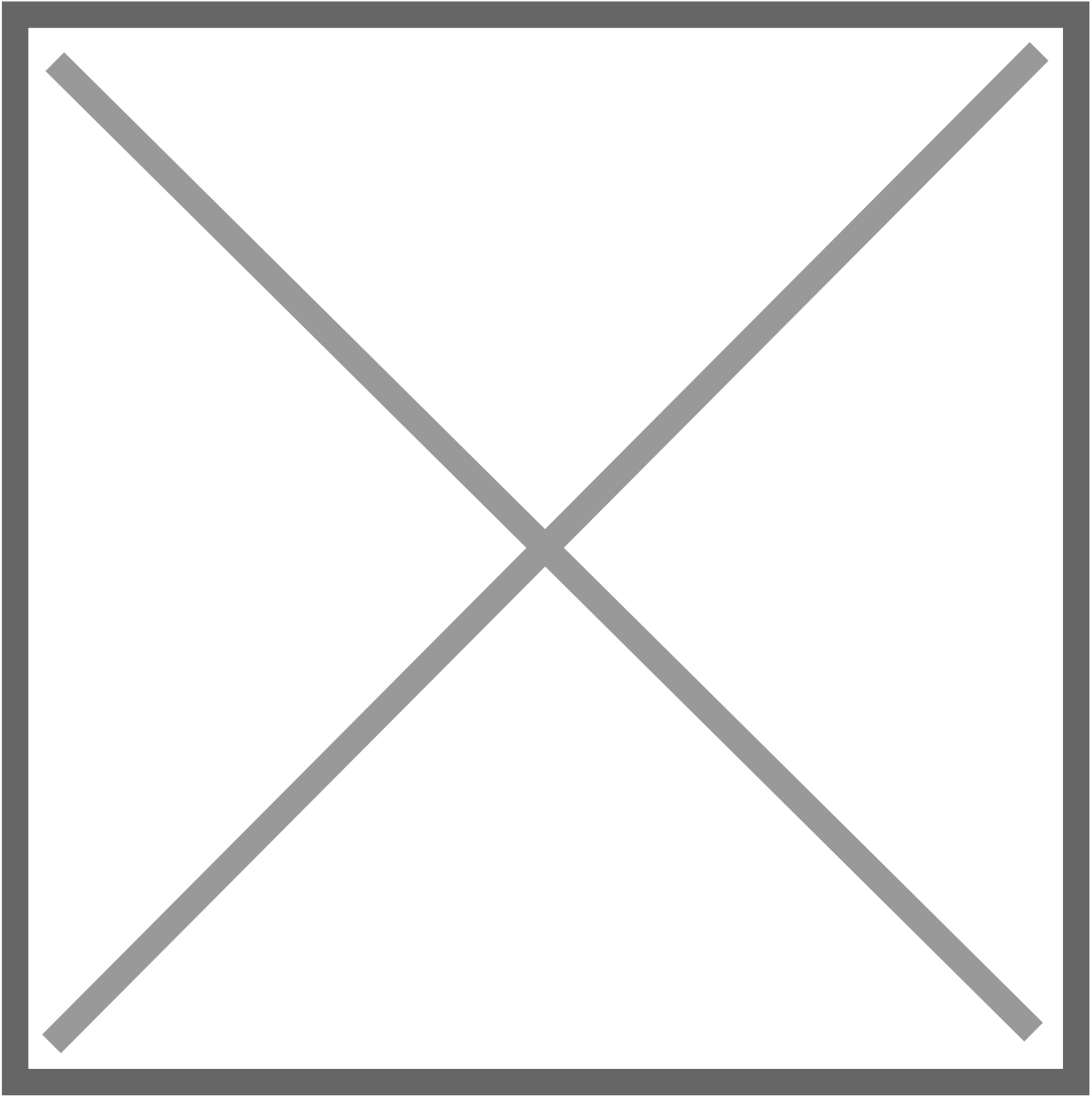
Damit Benutzer die entsprechenden Dashboards sehen können, ist als letzter Schritt notwendig, die definierten Rollen den gewünschten Benutzern zuzuordnen. Dies erfolgt über den Bereich Verwaltung.



Bearbeitet wird der gewünschte Benutzer über das Stift Symbol im rechten Bereich.

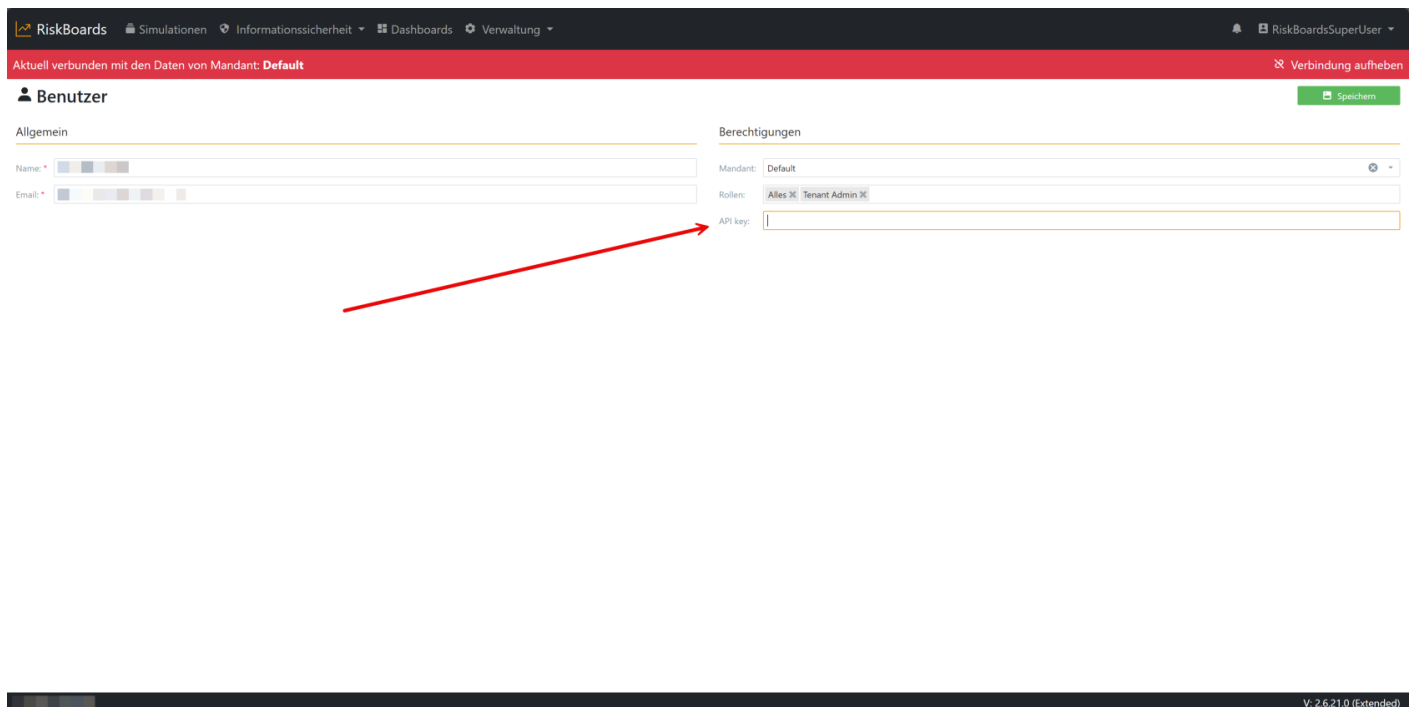


Im Bereich **Berechtigungen** ist bei **Rollen** die entsprechende Rolle oder auch mehrere auszuwählen.



API zum Abrufen von Dashboards

Bestimmte Daten aus RiskBoards können über eine API abgerufen werden (aktuell Dashboards). Hierzu muss im entsprechenden Benutzer ein API Key hinterlegt werden, dieser wird als Hash in der Datenbank gespeichert.



The screenshot shows the RiskBoards user management interface. The top navigation bar includes 'RiskBoards', 'Simulationen', 'Informationssicherheit', 'Dashboards', and 'Verwaltung'. The user is logged in as 'RiskBoardsSuperUser'. The main content area is titled 'Benutzer' and is divided into two sections: 'Allgemein' and 'Berechtigungen'. The 'Allgemein' section has input fields for 'Name' and 'Email'. The 'Berechtigungen' section has a dropdown for 'Mandant' (set to 'Default'), a dropdown for 'Rollen' (set to 'All' and 'Tenant Admin'), and an input field for 'API key'. A red arrow points to the 'API key' input field. A 'Speichern' (Save) button is visible in the top right corner of the form area. The footer of the page shows 'V. 2.6.21.0 (Extended)'.

Der Abruf der Dashboards erfolgt über ein GET mit folgenden beiden Header Informationen:

X-UserId: Die Id des jeweiligen Benutzers (in den meisten Fällen der Benutzername)

X-APIKey: der festgelegte API Key

Die URL zum Abruf der Dashboards ist:

<https://SERVERNAME/riskboards/dashboards/dashboards>

Beispiel Postman:

https://[redacted]/riskboards/dashboards/dashboards

GET https://[redacted]/riskboards/dashboards/dashboards

Params Authorization Headers (10) Body Scripts Tests Settings

Headers 8 hidden

Key	Value	Description
<input checked="" type="checkbox"/> X-Userid	[redacted]	
<input checked="" type="checkbox"/> X-APIKey	[redacted]	
Key	Value	Description

Body Cookies (1) Headers (10) Test Results

200 OK - 606 ms - 822.23 KB

JSON Preview Visualize

```

1 [
2   {
3     "Id": "0e8e8c1c-ea3e-4409-bc8f-7db74baa6377",
4     "Name": "OCC",
5     "Version": "V1.0",
6     "Description": null,
7     "Menu": false,
8     "SimulationMenu": false,
9     "SortOrder": 15,
10    "Default": false,
11    "AutoRefresh": 60,
12    "EnableExport": true,
13    "EnableAnalysing": false,
14    "Definition": "<Dashboard>\n\n <Title Visible=false Text=OCC />\n\n <DataSources>\n\n <SqlDataSource Name=OCC ComponentName=sqlDataSource1>\n\n <Connection
Name=OCC FzomAppConfig=true />\n\n <Query Type=SelectQuery Name=tblAuswertungOCC>\n\n <Tables>\n\n <Table Name=tblAuswertungOCC /
>\n\n </Tables>\n\n <Columns>\n\n <AllColumns Table=tblAuswertungOCC />\n\n </Columns>\n\n </Query>\n\n <Query Type=SelectQuery
Name=tblOCRLeesefehler>\n\n <Tables>\n\n <Table Name=tblOCRLeesefehler />\n\n </Tables>\n\n <Columns>\n\n <Column
Table=tblOCRLeesefehler Name=Artikelnummer />\n\n <Column Table=tblOCRLeesefehler
Name=Abnummer />\n\n </Columns>\n\n </Query>\n\n </DataSources>\n\n </Dashboard>\n\n"
  }
]

```

Die Rückgabe erfolgt als Json.

Beispiel Json:

```

[
  {
    "Id": "0e8e8c1c-ea3e-4409-bc8f-7db74baa6377",
    "Name": "OCC",
    "Version": "V1.0",
    "Description": null,
    "Menu": false,
    "SimulationMenu": false,
    "SortOrder": 15,
    "Default": false,
    "AutoRefresh": 60,
    "EnableExport": true,
    "EnableAnalysing": false,
    "Definition": ".....",
    "Statistic": true,
    "AssignedRoles": [
      "DashboardAccessGroup2"
    ],
    "ChannelsEnabled": false,
    "DefaultTags": null,
    "OptionalTags": null,
  }
]

```

```
"FilterTagSource": null,
"CreatedBy": null,
"Created": null,
"CodeltemWidgetOptionsPrepared": null,
"Updated": "2025-06-17T16:17:56.599032",
"UpdatedBy": "RiskBoardsSuperUser",
"DataKey": "1."
},
{
  "Id": "1b6f8abd-e9bc-4c38-a6c9-7413b590c6ae",
  "Name": "TestBE",
  "Version": null,
  "Description": null,
  "Menu": false,
  "SimulationMenu": false,
  "SortOrder": 10,
  "Default": false,
  "AutoRefresh": 0,
  "EnableExport": true,
  "EnableAnalysing": false,
  "Definition": ".....",
  "Statistic": true,
  "AssignedRoles": null,
  "ChannelsEnabled": false,
  "DefaultTags": null,
  "OptionalTags": null,
  "FilterTagSource": null,
  "CreatedBy": "RiskBoardsSuperUser",
  "Created": "2025-03-17T09:33:36.7017064",
  "CodeltemWidgetOptionsPrepared": null,
  "Updated": "2025-03-17T09:33:36.7017064",
  "UpdatedBy": "RiskBoardsSuperUser",
  "DataKey": "1."
}
]
```

Lizenz beantragen

<https://wf.somax.de/webhook/3f76b019-c035-4bb0-9190-5e90188b6b33/chat>