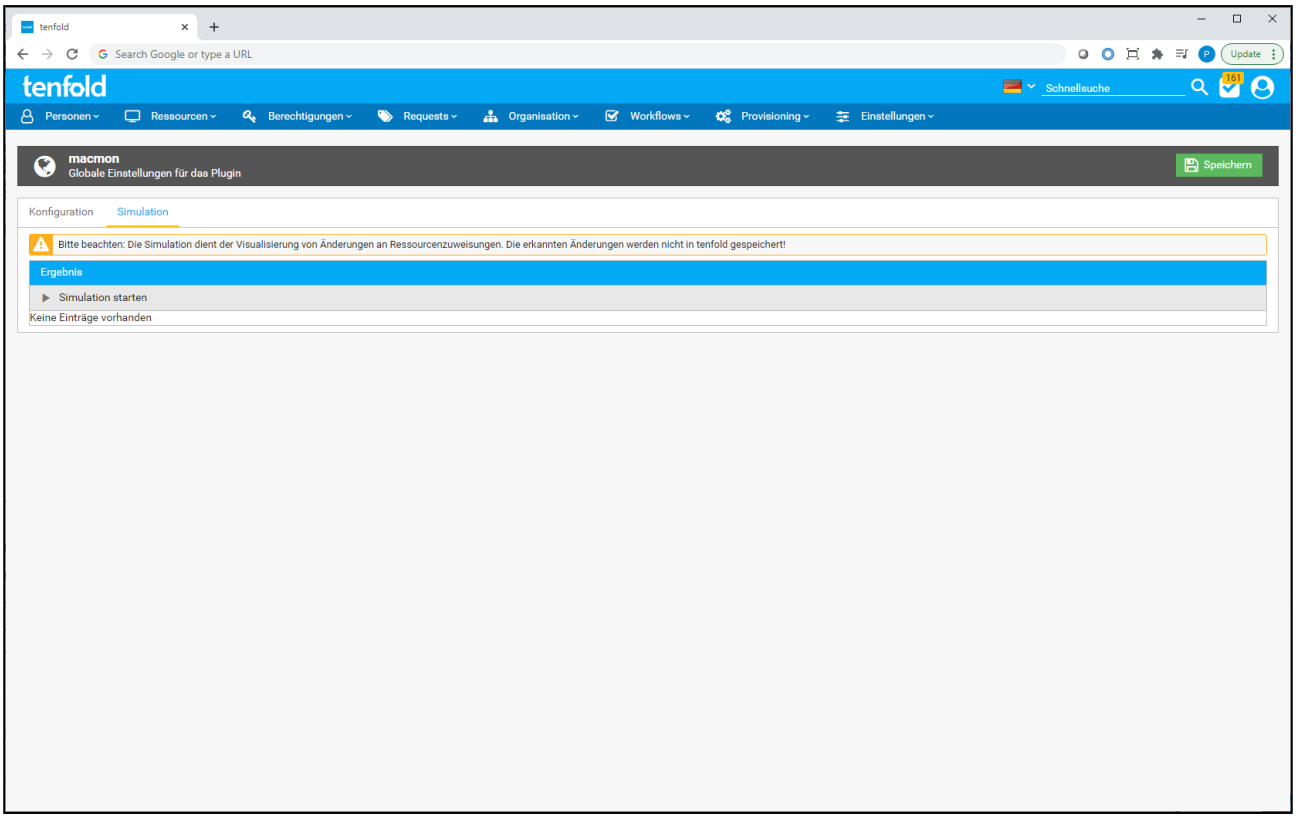
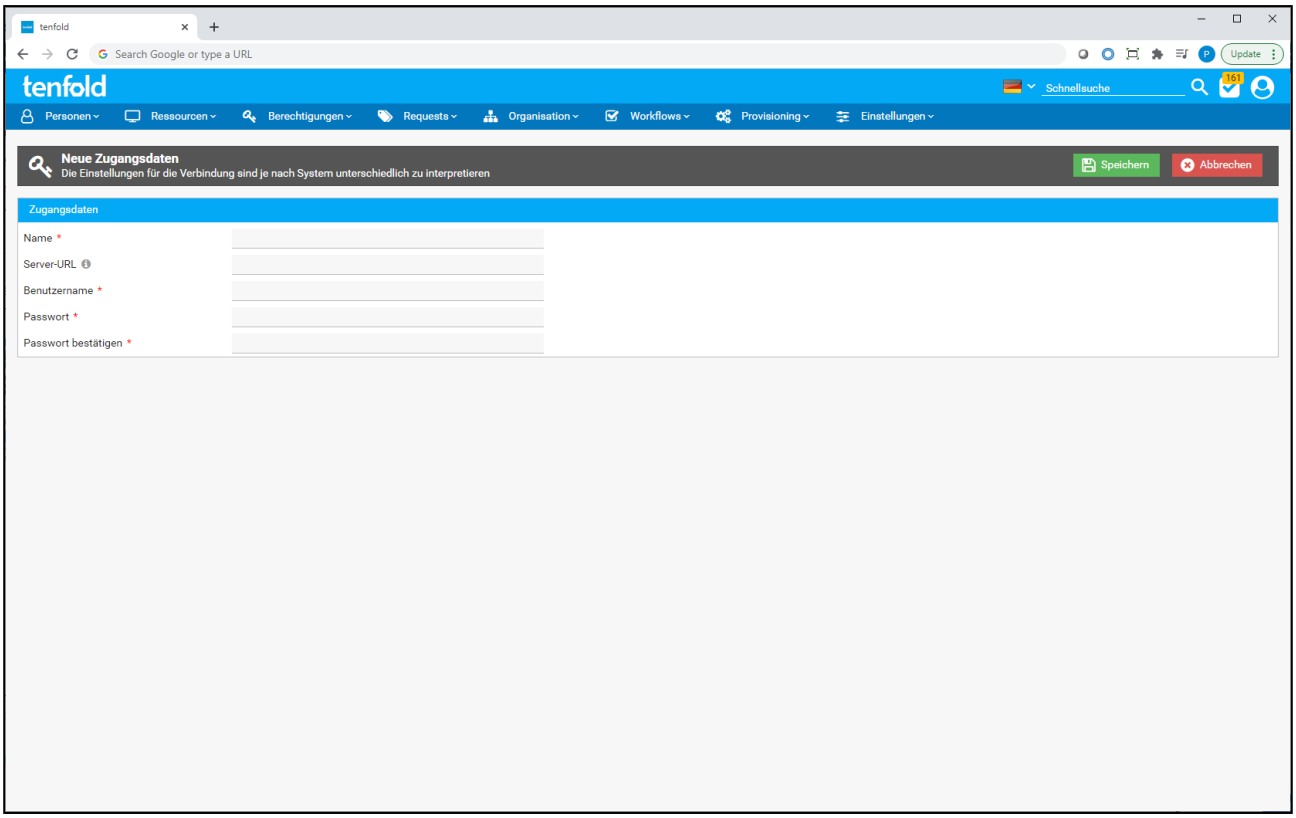
## Simulation




Im Karteireiter "Simulation" lässt sich eine Vorschau von allen Änderungen generieren, welche der tägliche Abgleichsjob durchführen würde.

## Zugangsdaten




Um den Zugriff auf den macmon-Dienst einzurichten, müssen Zugangsdaten für diesen definiert werden. Sie können neue Zugangsdaten für macmon anlegen indem Sie über das Menü auf die Seite Provisioning > Zugangsdaten wechseln. Dort können Sie im Auswahlmenü der Schaltfläche "Neu" "macmon" auswählen um neue Zugangsdaten anzulegen oder im Aktionsmenü bestehender Zugangsdaten "Bearbeiten" auswählen um diese anzupassen.
Folgende Einstellungen müssen hierbei definiert werden.

| Einstellung | Beschreibung |
|---|---|
| Name | Mit dieser Einstellung wird ein Name für die Zugangsdaten festgelegt, unter welchem die Zugangsdaten ausgewählt werden können. |
| Server URL | Der Basis URL für den macmon REST Dienst. Der URL muss hierbei in folgendem Format eingetragen werden: https://{Server-FQDN}/api/v{API-Version} |
| Benutzername | Der Benutzername des Benutzers mit welchem auf den macmon Dienst zugegriffen wird. |
| Passwort | Legt das Passwort fest mit welchem sich am macmon Dienst angemeldet wird. |
| Passwort wiederholen | Die Wiederholung des obigen Passwortes zur sicherheit. |

### Datenabgleich

Die Frequenz des Datenabgleichs lässt sich über das Menü Einstellungen > Jobs > verwaltung einrichten (siehe Jobs(see page 443)). Dort befindet sich nach der Installation des Plugins ein Job mit dem Namen "macmon Plugin - Sync". Durch die Zeiteinstellungen dieses Jobs kann konfiguriert werden in welcher Frequenz der Abgleich durchgeführt wird.

## 14.12 Microsoft 365 User Lifecycle

### 14.12.1 Allgemeines

In tenfold finden Sie weitreichende Möglichkeiten zur Verwaltung von Gruppenmitgliedschaften und Lizenzen im Microsoft 365-Umfeld. Genau wie für ein lokales Active Directory können Sie Benutzern in Microsoft 365 Gruppen und Lizenzen direkt oder über Profile im Azure Active Directory zuweisen. Dafür müssen die entsprechenden Objekte bereits in der Cloud existieren und in tenfold eingelesen werden. Dies kann entweder manuell durch die Microsoft 365 Administrator-Konsole geschehen oder, für Hybridumgebungen, über den Microsoft Active Sync.
Mit dem Microsoft-365-Plugin kann der Lebenszyklus von Microsoft-365-Benutzern direkt durch tenfold verwaltet werden. Das bedeutet:

- Benutzerkonten (reine Online-Benutzer oder Gastkonten) können angelegt werden.
- Stammdaten der Benutzerkonten können bei Personenänderungen aktualisiert werden.
- Konten können deaktiviert oder gelöscht werden.

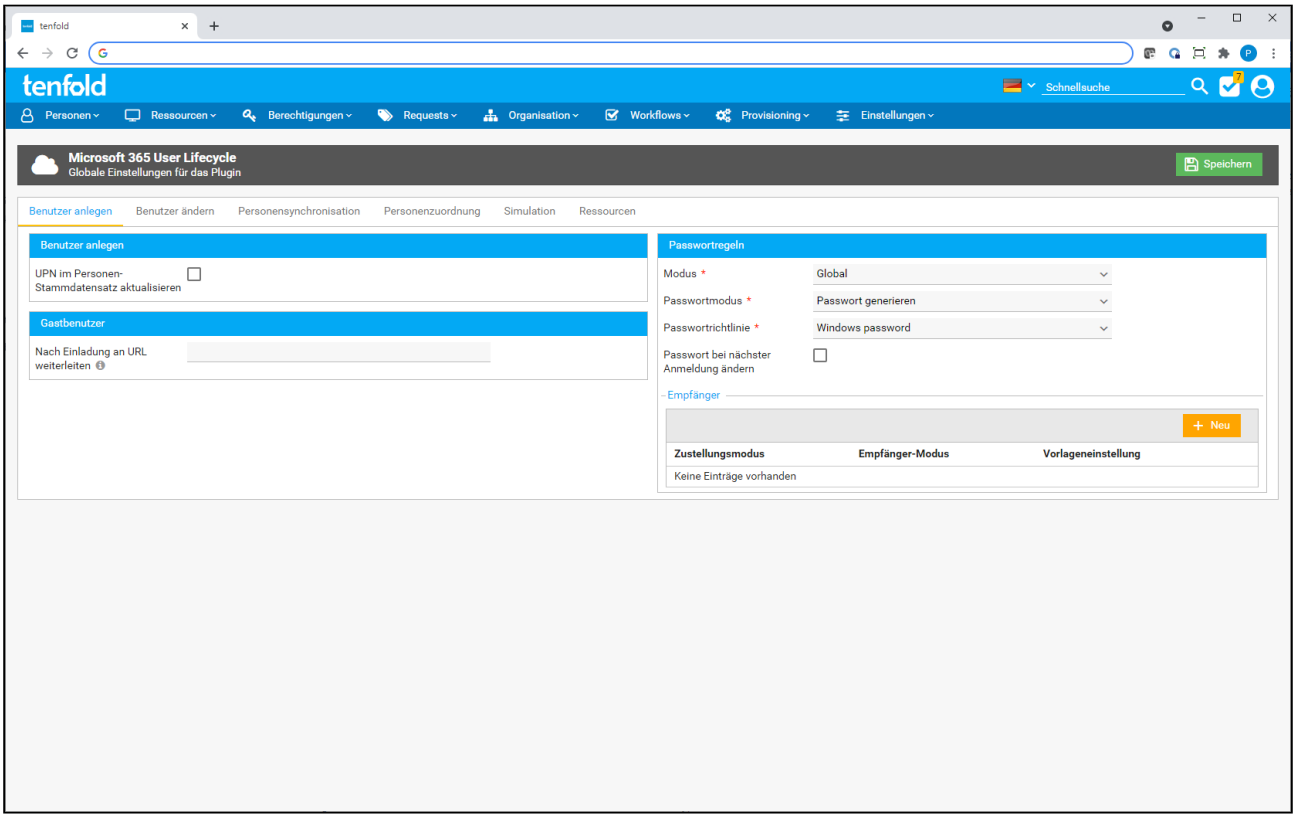
Benutzerkonten werden, wie beim Active Directory User Lifecycle auch, durch Ressourcen repräsentiert.

- Ein Konto wird in Microsoft 365 angelegt, wenn dem Benutzer eine entsprechende Ressource zugeordnet wird.
- Wird einer Person die Ressource entzogen, so wird das Benutzerkonto, je nach Einstellungen, deaktiviert oder gelöscht.
- Ändern sich die Personenstammdaten einer Person, der eine entsprechende Ressource zugeordnet ist, werden die Daten im Benutzerkonto angepasst.

Eine Ressource ist hierbei immer genau einem Mandanten zugeordnet, jedoch können zu jedem Mandanten mehrere Ressourcen angelegt werden. Dies dient dazu unterschiedliche Arten von Benutzerkonten pro Mandant abzubilden. Beispielsweise kann ein Mitarbeiter über ein normales Benutzerkonto und ein gesondertes Administrator-Konto verfügen. Anstatt hier in tenfold zwei Personen anzulegen können einfach derselben Person mehrere Ressourcen zugeordnet werden. Auch können hiermit für eine einzelne Person Benutzerkonten in unterschiedlichen Mandanten verwaltet werden.

### 14.12.2 Globale Einstellungen

> **Mandanten**
>
> Für die Verwendung des Microsoft 365 User Lifecycle Plugins ist die Einrichtung zumindest eines Mandanten unter *Einstellungen > Microsoft 365-Mandanten* zwingend erforderlich. Näheres finden Sie unter Einrichtung von Microsoft 365 Mandanten(see page 243).




Die globalen Einstellungen des Microsoft 365 User Lifecycle Plugins erreichen Sie unter *Provisioning > Plugins > Microsoft 365 User Lifecycle*. Dort können Sie die allgemeinen Einstellungen festlegen, welche für alle Benutzerkonto-Ressourcen gültig sind.
Diese Einstellungen sind in mehrere Karteireiter gegliedert:

- **Benutzer anlegen:** Legt fest, wie Benutzer in Microsoft 365 angelegt werden sollen.
- **Benutzer ändern:** Hier steuern Sie, wie Benutzer in Microsoft 365 aktualisiert werden sollen.
- **Personensynchronisation:** Regelt wie bestehende Benutzer von Microsoft 365 in tenfold importiert oder mit bestehenden Personen in tenfold abgeglichen werden sollen.
- **Personenzuordnung:** Hier können Sie konfigurieren, wie Microsoft 365-Benutzer bestehenden Personen in tenfold zugeordnet werden.
- **Simulation:** Hier kann ein Simulationslauf des Personenabgleichs durchgeführt werden, um zu sehen, welche Auswirkungen ein Abgleich mit den aktuellen Einstellungen hätte.
- **Ressourcen:** Hier können Sie Ressourcen anlegen, welche als Microsoft 365-Benutzerkontoressourcen dienen.

**Sperren und Löschen?**

Im Gegensatz zu einem lokalen Active Directory können in Microsoft 365 Benutzerkonten *nicht* in verschiedene Organisationseinheiten kategorisiert werden. Es entfallen daher die Einstellungsmöglichkeiten für diese Aktionen, da beim Sperren einer Ressourcenzuordnung das Konto in Microsoft 365 immer deaktiviert wird und beim Entfernen einer Zuordnung immer gelöscht

wird. Zur Einstellung, wie mit Gruppenmitgliedschaften beim Deaktivieren eines Kontos umgegangen werden soll, verwenden Sie an dieser Stelle die Einstellungen der Lifecycle-Phasen (siehe Lifecycle(see page 404)).

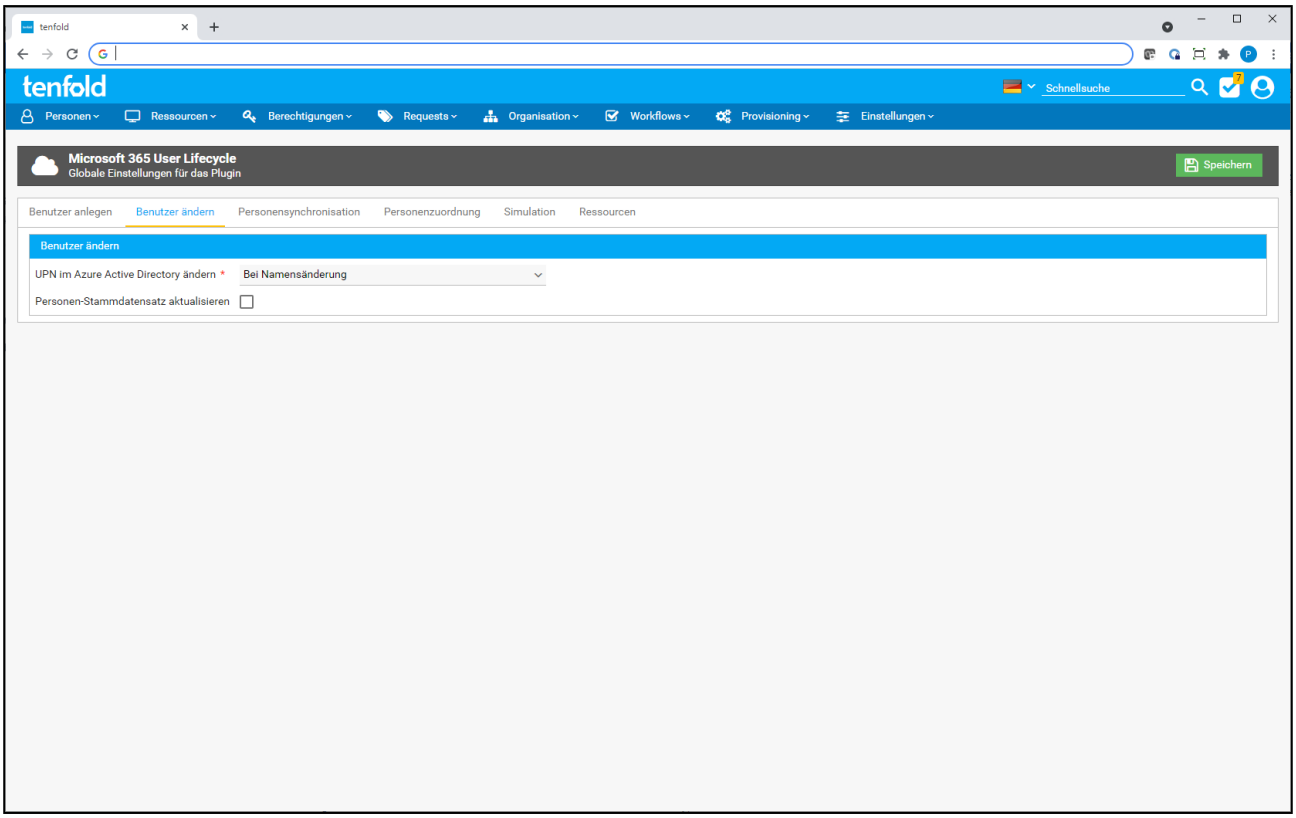
## Benutzer anlegen

Auf diesem Kartereiter finden Sie sämtliche Einstellungen zur Anpassung der Benutzeranlage in Microsoft 365. Folgende Einstellungen gibt es:

| Einstellung | Beschreibung |
|---|---|
| **Bereich "Benutzer anlegen"** | |
| UPN im Personen-Stammdatensatz aktualisieren | Wenn ein Konto in Microsoft 365 angelegt wird, wird für dieses ein neuer UPN generiert. Sollte in Ihren Personenstammdatensätzen das Feld "User Principal Name" vorkommen, so haken Sie diese Einstellung an, wenn Sie möchten, dass der hier generierte UPN in dieses Feld übertragen wird. |
| **Bereich "Gastbenutzer"** | |
| Nach Einladung an URL weiterleiten | Geben Sie hier einen URL an, an den die Gastbenutzer weitergeleitet werden, sobald Sie Ihre Einladung abgeschlossen haben. |

Zusätzlich zu diesen Einstellungen finden Sie im Bereich "Passwortregeln" auch die Einstellungen, die definieren, wie Passwörter für neue Benutzer angelegt, gesetzt und versendet werden sollen. Hierbei handelt es sich um allgemeine Einstellungen, wie Sie sie an mehreren Stellen in tenfold finden. Eine Erklärung zu diesen Einstellungen finden Sie unter Erzeugung von Passwörtern(see page 648).

## Benutzer ändern

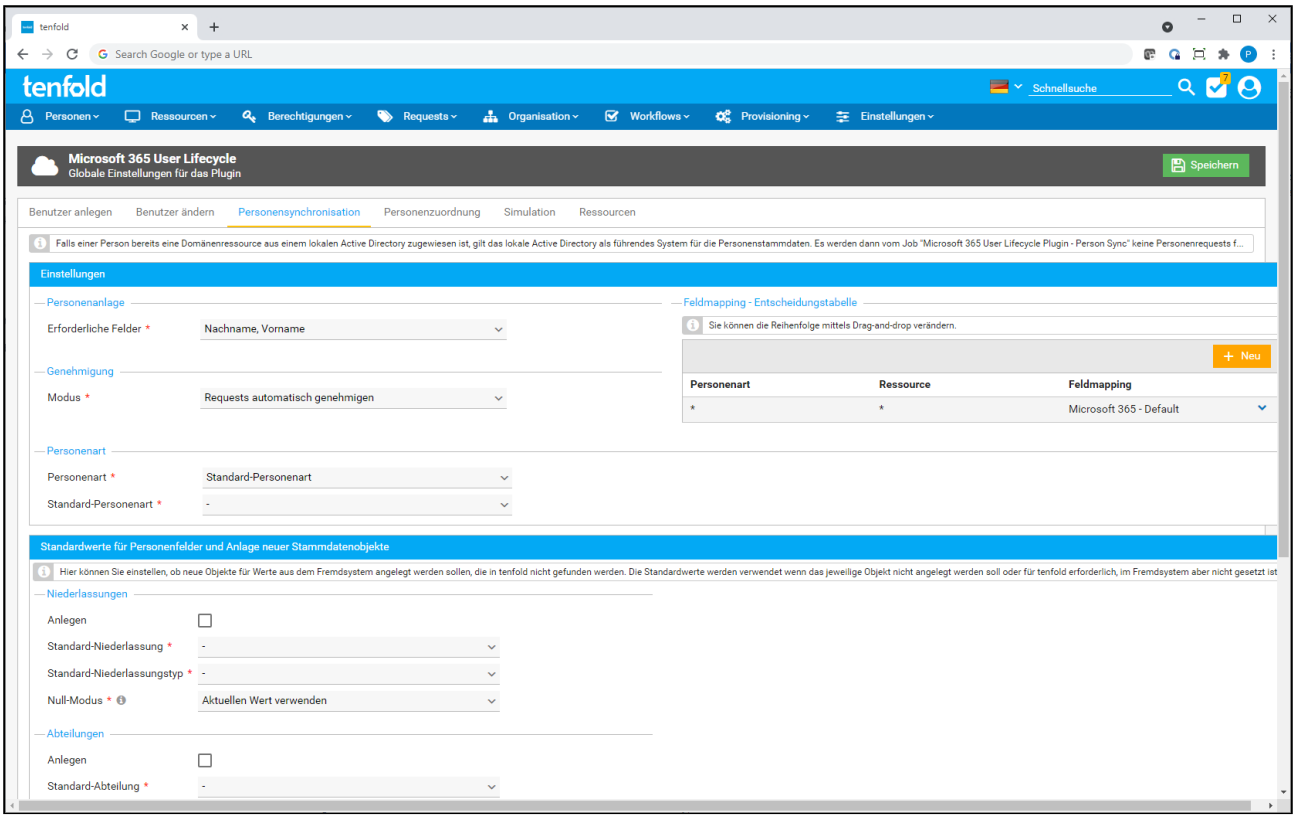



Auf diesem Karteireiter befinden sich Einstellungen zur Aktualisierung von Benutzerkonten bei Personenänderung in tenfold. Folgende Einstellungen stehen Ihnen zur Verfügung:

| Einstellung | Beschreibung |
|---|---|
| **Bereich "Benutzer ändern"** | |
| UPN im Azure Active Directory ändern | Mit dieser Einstellung kann bestimmt werden, ob und wann der UPN im Azure Active Directory angepasst werden soll, sollten sich Personenänderung in tenfold ergeben.<br>• **Nie:** Änderungen in tenfold lösen niemals eine Änderung des UPN aus.<br>• **Bei Namensänderung:** Sollten sich die Felder "Vorname" oder "Nachname" des Personenstammdatensatzes ändern, erzeugt tenfold einen neuen UPN und überträgt ihn in das AAD.<br>• **Bei manueller Änderung:** Sollte sich das Feld "User Principal Name" in tenfold ändern, wird die Änderung in das AAD übertragen.<br>• **Bei Stammdatenänderungen:** Bei allen Stammdatenänderungen wird ein UPN generiert. Sollte dieser sich zum aktuellen UPN unterscheiden, so wird der neue UPN ins AAD übertragen. |

| Einstellung | Beschreibung |
|---|---|
| **Bereich "Benutzer ändern"** | |
| Personen-Stammdatensatz aktualisieren | Mit dieser Einstellung bestimmen Sie, ob bei Änderung des UPN durch die oben getroffene Einstellung, der UPN im Stammdatensatz von tenfold aktualisiert werden soll. Verwenden Sie diese Einstellung, wenn Sie das Feld "User Principal Name" in Ihren Stammdatensätzen verwenden. |

## Personensynchronisation




Im Karteireiter "Personensynchronisation" finden Sie sämtliche Einstellungen, welche beeinflussen, wie eine Benutzerkonto von Microsoft 365 nach tenfold übertragen wird. Dies geschieht, in einstellbaren Intervallen, durch den Job "Microsoft 365 Plugin - Person Sync", welcher mit Installation des Plugins angelegt wird. Nähere Informationen zur Einrichtung von Jobs finden Sie unter Jobs(see page 443).
Außerdem finden Sie hier die Einstellung des Feldmappings, welches verwendet wird, um eine Verbindung zwischen tenfold-Personenfeldern und Attributen in Azure Active Directory herzustellen. Dies gilt sowohl für den Import nach tenfold als auch für den Export in das AAD.
Im Bereich "Einstellungen" finden Sie zunächst folgende Optionen:

| Einstellung | Beschreibung |
|---|---|
| **Abschnitt "Personenanlage"** | |

| | |
|---|---|
| Erforderliche Felder | Mit dieser Einstellung legen Sie fest, über welche Felder ein Personenstammdatensatz, nach Anwendung des Feldmappings aus dem Azure Active Directory, verfügen muss, um in tenfold angelegt zu werden. Verfügt ein Konto nicht über die erforderlichen Felder, so wird die Person in tenfold nicht angelegt. Verwenden Sie diese Einstellung, um zu vermeiden, dass technische Konten, wie Raumkonten oder Druckerkonten, in tenfold als Person angelegt werden.<br>Folgende Einstellungsmöglichkeiten stehen hier zur Verfügung:<br>• Nachname, Vorname: Es müssen im Stammdatensatz Nachname und Vorname enthalten sein.<br>• Nachname: Es muss der Nachname im Stammdatensatz enthalten sein.<br>• Code Snippet: Es wird ein Code Snippet aufgerufen, welches entscheidet, ob der Benutzer als Person angelegt werden soll. |
| Code Snippet | Dieses Code Snippet wird aufgerufen, wenn in der Einstellung "Erforderliche Felder" die Auswahl "Code Snippet" gewählt wurde. Das Code Snippet erhält das vollständig befüllte Personenobjekt als variable "Person" und muss den Wert "true" zurückliefern, wenn die Person angelegt werden soll und "false," wenn nicht. Hinweis: Sie erhalten nur Zugriff auf die bereits gemappten Personendaten, wenn sie durch das Feldmapping erzeugt wurden. Ein direkter Zugriff auf die Daten in Azure AD ist nicht möglich. |
| **Abschnitt "Genehmigung"** | |
| Modus | Hiermit können Sie festlegen, wie mit den aus der Personensynchronisation erzeugten Requests verfahren werden soll. Sie haben folgende Auswahlmöglichkeiten:<br>• **Requests automatisch genehmigen:** Die entstandenen Requests werden automatisch genehmigt. Dadurch werden Provisionierungsschritte durchgeführt und die aus dem Abgleich entstandenen Änderungen werden, je nach Einstellung, in andere Systeme propagiert.<br>• **Requests als abgeschlossen anlegen:** Die Requests werden ohne Provisionierung abgeschlossen. Dadurch wird der Stammdatensatz in tenfold aktualisiert, weitere Änderungen werden jedoch nicht durchgeführt. |
| **Abschnitt "Personenart"** | |

| | |
|---|---|
| Personenart | Mit dieser Einstellung wird festgelegt, welche Personenart Personen erhalten sollen, die aus Microsoft 365 angelegt werden. Sie haben folgende Auswahlmöglichkeiten:<br>• **Standard-Personenart:** Alle Personen erhalten dieselbe voreingestellte Personenart.<br>• **Entscheidungstabelle:** Sie können eine Entscheidungstabelle anlegen, die bestimmt, welche Personenart Personen erhalten.<br>• **Code Snippet:** Sie können ein Code Snippet angeben, welches die Personenart bestimmt. |
| Standard-Personenart | Wurde in der obigen Einstellung "Standard-Personenart" ausgewählt, so wird hier die Personenart festgelegt, die alle Personen erhalten, die importiert werden. Wurde die Auswahl "Entscheidungstabelle" getroffen, wird hiermit eingestellt, welche Personenart eine Person erhalten soll, wenn in der Entscheidungstabelle keine zutreffende Zeile gefunden wurde. |
| Entscheidungstabelle | In dieser Tabelle können Sie entscheiden, welche Personenart eine Person in tenfold erhalten soll. Beim Import prüft tenfold diese Tabelle, Zeile für Zeile, und verwendet die Personenart der ersten Zeile, deren Kriterien erfüllt werden. Fügen Sie der Tabelle eine neue Zeile mittels der Schaltfläche "Neu" hinzu. Sie können die Reihenfolge der Zeilen durch Drag & Drop verändern. In jeder Zeile haben Sie folgende Einstellungsmöglichkeiten:<br>• **Auswertungsmodus:** Legt fest, ob ein Wert aus dem Azure AD ausgewertet werden soll oder ob ein Code Snippet verwendet werden soll.<br>• **Feld:** Wurde im Auswertungsmodus die Einstellung "Wert" getroffen, so kann hier das Feld "User Principal Name" oder "Typ" ausgewählt werden.<br>• **Überprüfungsart:** Hiermit können Sie festlegen, auf welche Art der User Principal Name überprüft wird.<br>• **Wert:** Dies ist der Vergleichswert für den User Principal Name.<br>• **Typ:** Wurde bei "Feld" der Wert "Typ" ausgewählt, so kann hier entschieden werden, auf welchen Typ von Benutzer die Zeile zutrifft.<br>• **Code Snippet:** Dieses Code Snippet wird ausgeführt, um zu prüfen, ob die Zeile zutrifft.<br>• **Personenart:** Legt das Ergebnis der Zeile fest. Diese Personenart wird ausgewählt, wenn die Zeile auf einen Benutzer zutrifft.<br>Das Code Snippet erhält die Variable "user", mit welcher auf die Daten des Benutzerkontos im Azure AD zugegriffen werden kann (Beispiel: user.givenName) und muss "true" zurückliefern, damit die Zeile als erfüllt gilt. |

| | |
|---|---|
| Bereits vorhandene Personen | Mit dieser Einstellung wird bestimmt, wie mit der Personenart bereits vorhandener Personen umgegangen werden soll. Sie haben folgende Optionen:<br>• **Decision Table und Standard-Personenart berücksichtigen:** Die Entscheidungstabelle wird ausgewertet. Sollte kein passender Eintrag gefunden werden, wird die Personenart der existierenden Person mit der gewählten Standardpersonenart überschrieben.<br>• **Nur Decision-Table berücksichtigen, keine Änderung ohne passenden Eintrag:** Die Entscheidungstabelle wird geprüft. Sollte kein passender Eintrag gefunden werden, so bleibt die aktuelle Personenart der existierenden Person unverändert.<br>• **Personenart nicht verändern:** Die Personenarten von existierenden Personen bleiben vom Abgleich in jedem Fall unverändert.<br>**Achtung:** Für Personen, welche durch den Abgleich neu angelegt werden, gilt immer sowohl die Entscheidungstabelle, also auch die Standardpersonenart, sollte kein passender Eintrag gefunden werden. |
| Code Snippet | Legt ein Code Snippet fest, welches die gewünschte Personenart zurückliefern muss. Es erhält die Variable "user," um damit die Daten aus dem Azure Active Directory abfragen zu können. Zum Beispiel: user.givenName |
| **Abschnitt "Feldmapping - Entscheidungstabelle"** | |

| | |
|---|---|
| Entscheidungstabelle | Mit dieser Entscheidungstabelle wird festgelegt, welches Feldmapping für die betroffenen Personen/Benutzer verwendet werden soll, um diese in das entsprechende Gegenstück umzuwandeln. Diese Entscheidungstabelle wird sowohl ausgewertet, wenn eine Person in tenfold verändert wurde, um die Attributsänderungen im Azure AD zu ermitteln als auch beim Import nach tenfold, um die notwendigen Personenänderungen festzustellen.<br>In jeder Zeile können Sie eine Kombination aus Personenart oder Ressource festlegen, um zu ermitteln, ob die Zeile zutrifft. Die erste Zeile, auf welche beide Einstellungen zutreffen, wird verwendet. Alternativ können Sie in einer Zeile auch ein Code Snippet hinterlegen, um zu prüfen, ob die Zeile auf eine Person/einen Benutzer zutrifft.<br>Das Code Snippet erhält folgende Parameter:<br>• **personType:** Die Personenart der Person, welche in das AAD übertragen werden soll (nur Export ins AAD).<br>• **service:** Die Ressource, welche das Benutzerkonto in tenfold darstellt (nur Export ins AAD).<br>• **personMasterdata:** Der Stammdatensatz, der ins AAD zu übertragenden Personen (nur Export ins AAD).<br>• **request:** Der Request, der die Änderungen ausgelöst hat (nur Export ins AAD).<br>• **user:** Die Benutzerdaten des Kontos im AAD (nur Import nach tenfold).<br>Das Code Snippet muss "true" zurückliefern, damit die Zeile als erfüllt gilt. |

**Active Directory-Benutzer**

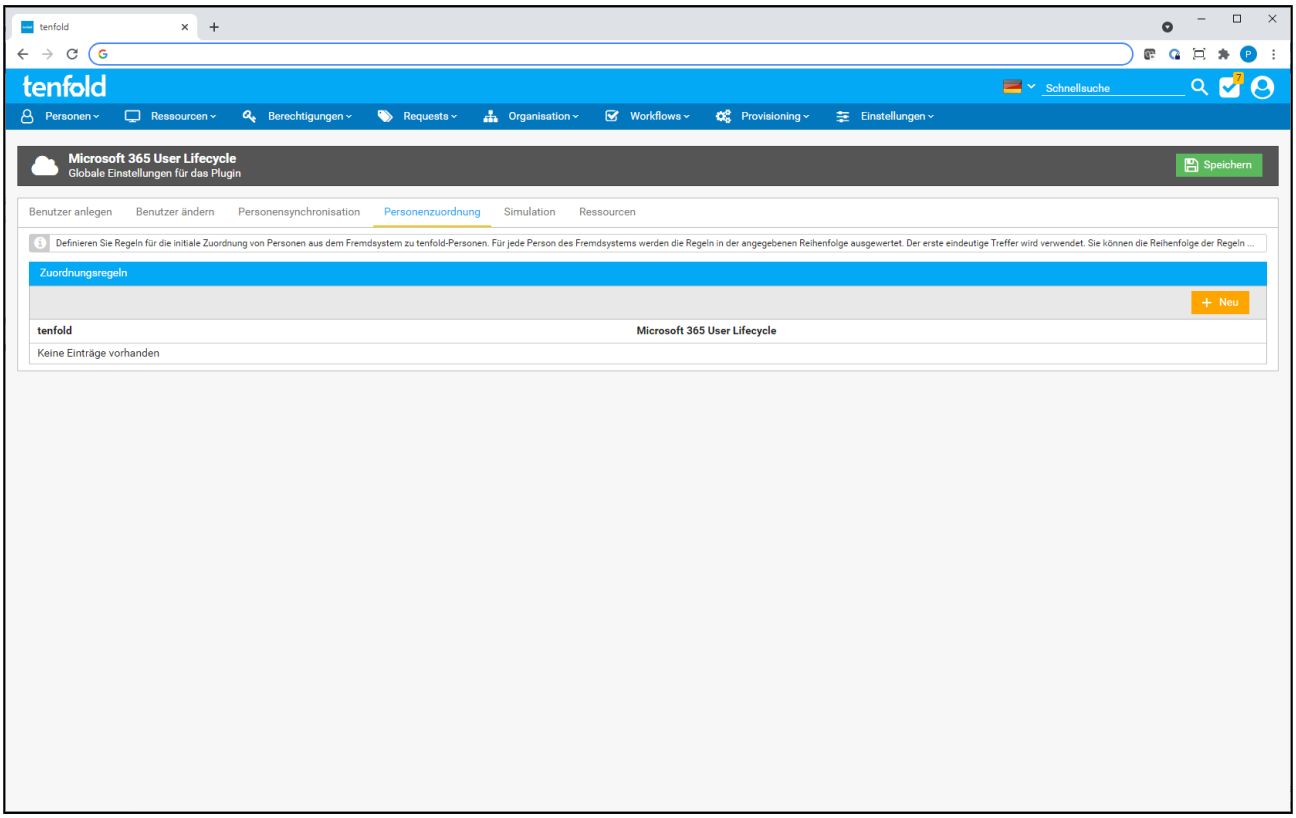
Das Active Directory User Lifecycle Plugin hat Vorrang vor dem Microsoft 365 User Lifecycle Plugin. Personen, die bereits durch das Active Directory Plugin abgeglichen werden (alle Personen mit Zuweisung einer Active Directory Ressource), werden daher vom Microsoft 365 User Lifecycle Plugin beim Import ignoriert und deren Daten werden nicht abgeglichen. Benutzer, die im Azure Active Directory ursprünglich gefunden werden, werden jedoch normal angelegt.

Im Bereich "Standardwerte für Personenfelder und Anlage neuer Stammdatenobjekte" können Sie konfigurieren, wie in tenfold mit Stammdatenobjekten verfahren werden soll, die in den importierten Personen nach dem Feldmapping aufscheinen und die nicht in tenfold vorhanden sind.
Für jede Art von Stammdatenobjekten (Abteilung, Niederlassung, etc.), welche in den verwendeten Feldmappings vorkommen, finden Sie einen Abschnitt vor, in welchem Sie einstellen können, wie mit dieser Art von Stammdatenobjekt umzugehen ist. Sie haben hierbei folgende Einstellungsmöglichkeiten:

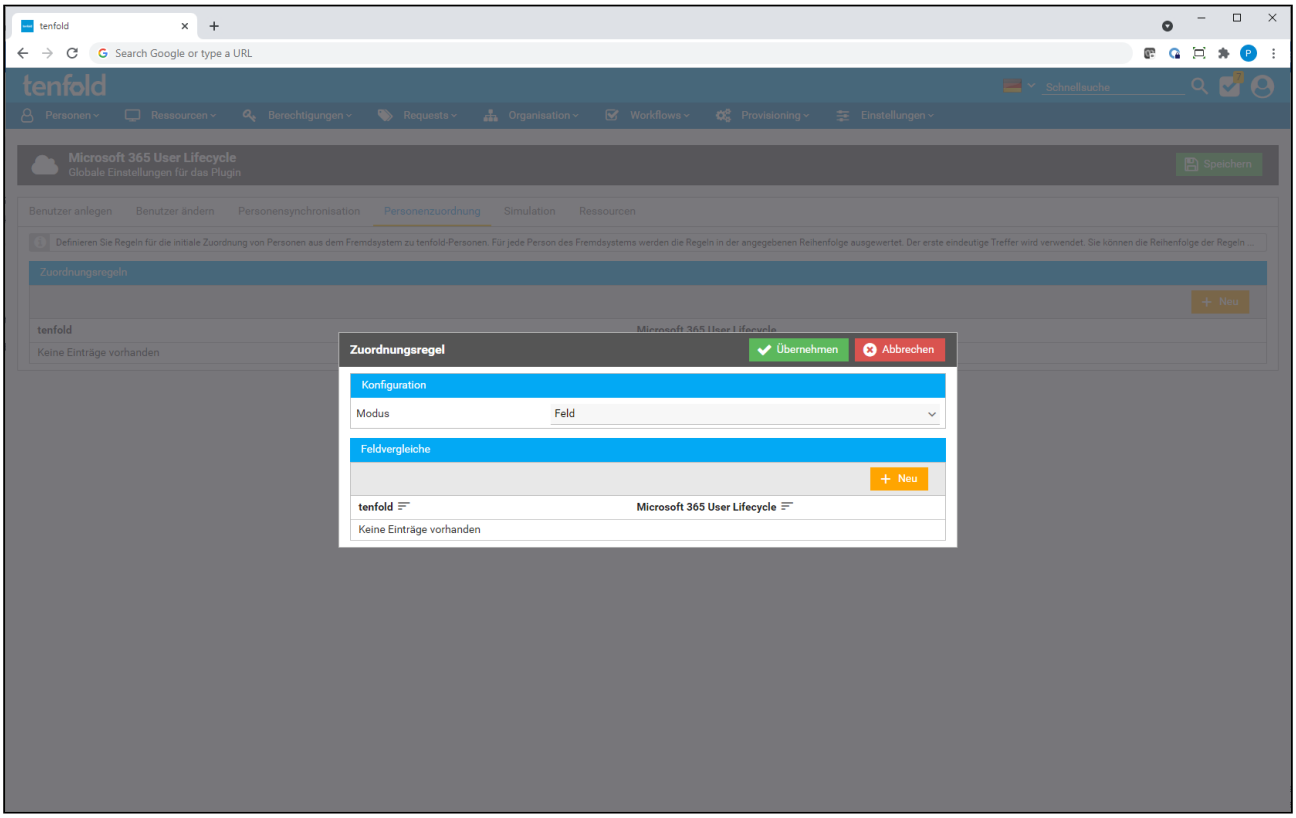
| Einstellung | Beschreibung |
|---|---|
| Anlegen | Mit dieser Einstellung legen Sie fest, ob das Stammdatenobjekt angelegt werden soll, wenn es in tenfold nicht gefunden werden konnte. Ist diese Einstellung angehakt, so wird das gefundene Objekt in tenfold angelegt. Ist diese Einstellung nicht angehakt, wird das Objekt nicht angelegt und die importierte Person erhält stattdessen den eingestellten Standardwert. |

| Einstellung | Beschreibung |
| --- | --- |
| Standard-<Objektart> | Mit dieser Einstellung legen Sie fest, welches Objekt dieser Art verwendet werden soll, wenn der importierte Wert in tenfold nicht gefunden wurde und auch nicht angelegt werden soll. Für manche Objektarten gibt es mehrere Standardwerteinstellungen. Die erste Einstellung bezieht sich hierbei immer auf den Standardwert, der bei Bedarf der Person zugeordnet wird.<br>Für Manche Objektarten können mehrere Standardwerteinstellungen vorhanden sein. Die erste Einstellung bezieht sich immer auf das Objekt, welches der Person zugeordnet werden soll. Die weiteren Einstellungen legen fest, mit welchen Bezugsobjekten die Objekte angelegt werden sollen.<br>**Beispiel:** Eine Niederlassung hat einen Niederlassungstyp. Sollte es erforderlich sein, eine neue Niederlassung durch den Import anzulegen, so kann hier festgelegt werden, welchen Niederlassungstypen eine neu angelegte Niederlassung erhalten soll, sollte dies aus dem Import nicht ersichtlich sein.<br>**Achtung: Bezugsobjekte werden nach der Anlage eines Objektes nicht mehr aktualisiert. Bei Niederlassungen wird, zum Beispiel, der Wert für "Standard-Niederlassungstyp" nur bei der Anlage neuer Niederlassungen verwendet. Sollte zu einem späteren Zeitpunkt dieselbe Niederlassung mit einem anderen Niederlassungstyp aufscheinen, so wird diese nicht mehr angepasst.** |
| Null-Modus | Diese Einstellung legt fest, ob bei einem Leerwert im Fremdsystem der aktuelle Wert der Person in tenfold beibehalten werden soll (oder leer ist, im Falle von Neuanlagen) oder, ob stattdessen der eingestellte Standardwert verwendet werden soll. |

## Personenzuordnung



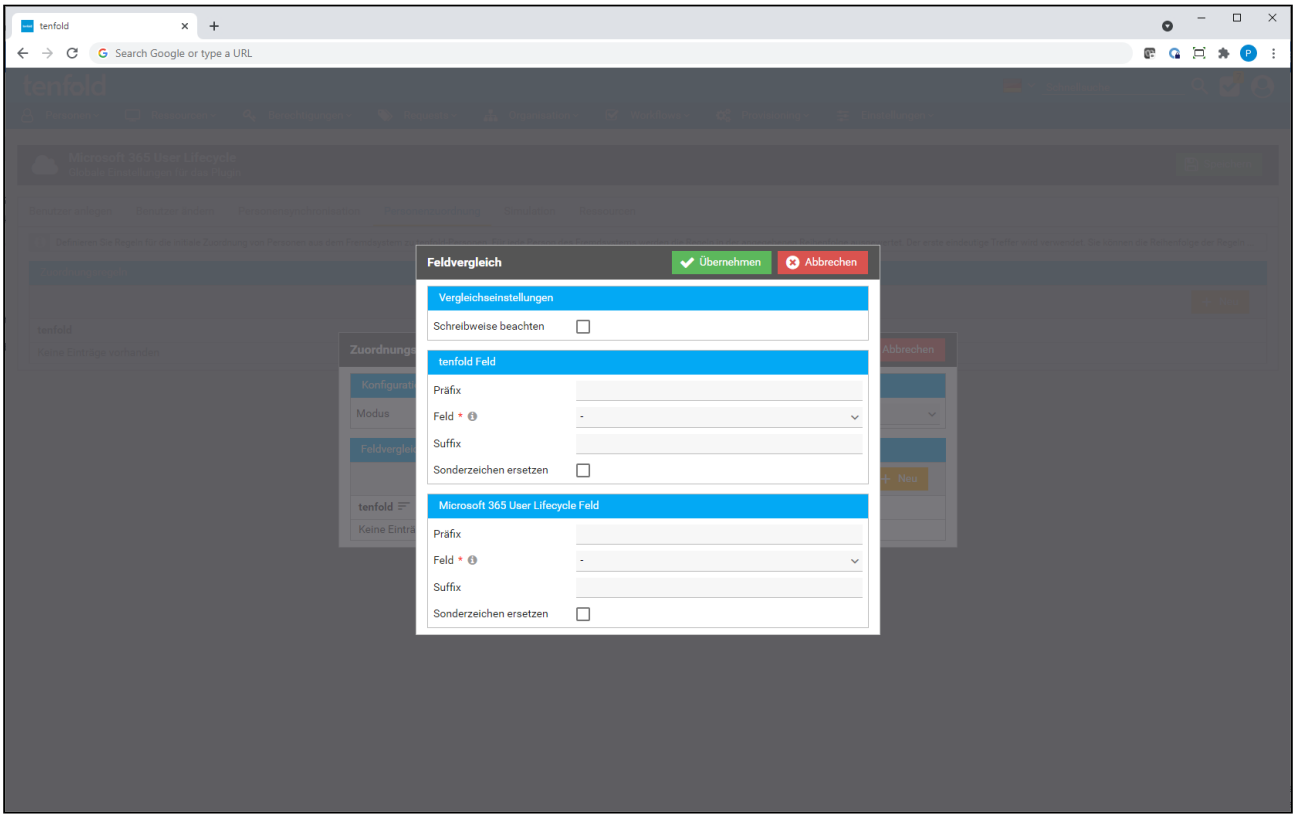

Auf diesem Kartereiter wird festgelegt, wie Benutzerkonten in Microsoft 365 bestehenden tenfold-Personen zugeordnet werden können.
Hierfür können Sie ein Regelwerk aus mehreren Regeln festlegen, die der Reihe nach auf die bestehenden Personen angewandt werden. Sollte eine der Regeln auf eine Person in tenfold zutreffen, so wird die ermittelte Person durch den Abgleich aktualisiert und es wird ihr die entsprechende Microsoft 365-Kontoressource zugeordnet, sofern sie diese noch nicht hat. Sollte keine Person in tenfold gefunden werden, auf die eine der Regeln zutrifft, wird eine neue Person in tenfold mit den ermittelten Daten aus dem Feldmapping angelegt und es wird ihr zugleich die Kontoressource zugewiesen.
Um eine neue Regel hinzuzufügen, betätigen Sie die Schaltfläche "Neu". Es öffnet sich daraufhin ein Dialog zur Konfiguration der neuen Regel.




Zunächst haben Sie im Bereich "Konfiguration" die Einstellung "Modus". Mit dieser Legen Sie die Art fest, wie die Prüfung durchgeführt werden soll.

| Modus | Beschreibung |
|---|---|
| Feld | Die Prüfung findet durch eine Reihe von Feldvergleichen statt. Welche Felder verglichen werden sollen, können Sie im Bereich "Feldvergleiche" einstellen. Dieser wird allerdings nur sichtbar, wenn der Modus "Feld" gewählt wurde. |
| Code Snippet | Die Prüfung findet durch ein Code Snippet statt. Das Code Snippet kann im Bereich "Code Snippet" eingegeben werden. Dieser ist allerdings nur sichtbar, wenn dieser Modus ausgewählt wurde. |

Haben Sie den Modus "Feld" ausgewählt, so können Sie im Bereich "Feldvergleiche" ein oder mehrere Felder einstellen, die verglichen werden. Sollten Sie mehrere Felder auswählen, müssen alle Feldvergleiche positiv sein, damit diese Regel als erfüllt gilt. Um einen neuen Feldvergleich einzufügen, klicken Sie auf die Schaltfläche "Neu". Es öffnet sich daraufhin ein weiterer Dialog, in welchem Sie einstellen können, wie der Feldvergleich stattfinden soll.




Folgende Einstellungen finden Sie an dieser Stelle, um zu konfigurieren, wie der Vergleich stattfinden soll:

| Einstellung | Beschreibung |
|---|---|
| **Bereich "Vergleichseinstellungen"** | |
| Schreibweise beachten | Mit dieser Einstellung wird festgelegt, ob die Groß-/Kleinschreibung der Felder für den Vergleich beachtet werden soll oder nicht. |
| **Bereich "tenfold Feld"** | |
| Präfix | Mit dieser Einstellung können Sie dem Feld in tenfold zu Vergleichszwecken ein Präfix voranstellen. Sollte das Feld in Microsoft 365 beispielsweise immer mit "Adm" beginnen, nach tenfold jedoch ohne "Adm" importiert werden, können Sie dieses Präfix hier angeben, damit der Vergleich erfolgreich stattfinden kann. |
| Feld | Wählen Sie hier das Feld in tenfold aus, welches für den Vergleich herangezogen werden soll. |
| Suffix | Ähnlich dem Präfix kann hier ein Suffix angegeben werden, sollte das Feld in Microsoft 365 immer mit einem gewissen Wert enden, in tenfold jedoch nicht. |

| | |
|---|---|
| Sonderzeichen ersetzen | Ist diese Einstellung aktiv werden Sonderzeichen, wie zum Beispiel Umlaute, im tenfold-Feld für den Vergleich ersetzt. Sollte im tenfold-Feld zum Beispiel "Ü" stehen, wird für den Vergleich die Zeichenkette "Ue" herangezogen. |
| **Bereich "Microsoft 365 User Lifecycle Feld"** | |
| Präfix | Mit dieser Einstellung können Sie dem Feld in Microsoft 365 zu Vergleichszwecken ein Präfix voranstellen. Sollte das Feld in tenfold beispielsweise immer mit "Adm" beginnen, nicht jedoch in Microsoft-365, können Sie dieses Präfix hier angeben, damit der Vergleich erfolgreich stattfinden kann. |
| Feld | Wählen Sie hier das Feld in Microsoft 365 aus, welches für den Vergleich herangezogen wird. |
| Suffix | Ähnlich dem Präfix kann hier ein Suffix angegeben werden, sollte das Feld in tenfold immer mit einem gewissen Wert enden, in Microsoft-365 jedoch nicht. |
| Sonderzeichen ersetzen | Ist diese Einstellung aktiv, werden Sonderzeichen wie Umlaute im tenfold-Feld für den Vergleich ersetzt. Sollte im Microsoft 365-Feld zum Beispiel "Ü" stehen, wird für den Vergleich die Zeichenkette "Ue" herangezogen. |

Für den Vergleich werden also immer zwei Werte erzeugt, bestehend aus "<Präfix><Feld><Suffix>" und diese werden daraufhin anhand aller Einstellungen verglichen.
Sollten Sie den Modus "Code Snippet" gewählt haben, wird anstatt der Feldvergleiche ein Code Snippet durchgeführt. Dieses erhält als Parameter den Wert "externalUser", mit welchem Sie auf die Felder in Microsoft 365 zugreifen können. Mit "externalUser.givenName" erhalten Sie zum Beispiel den Vornamen des Benutzers in Microsoft 365. Außerdem erhalten Sie eine liste aller Personen aus tenfold, mittels der Variable "persons". Für eine erfolgreiche Zuordnung muss eine der Personen aus dieser Liste zurückgegeben werden.

**Beispiel: Matching durch UPN**

```
persons.find { person -> person.masterdata.userPrincipalName ==
                    externalUser.userPrincipalName }
```

**Matching durch Personalnummer mit führenden 0 in Microsoft 365 aber nicht in tenfold**

```
persons.find { person -> person.masterdata.staffNumber ==
                        externalUser.employeeNumber.replaceFirst(/0+/, '') }
```

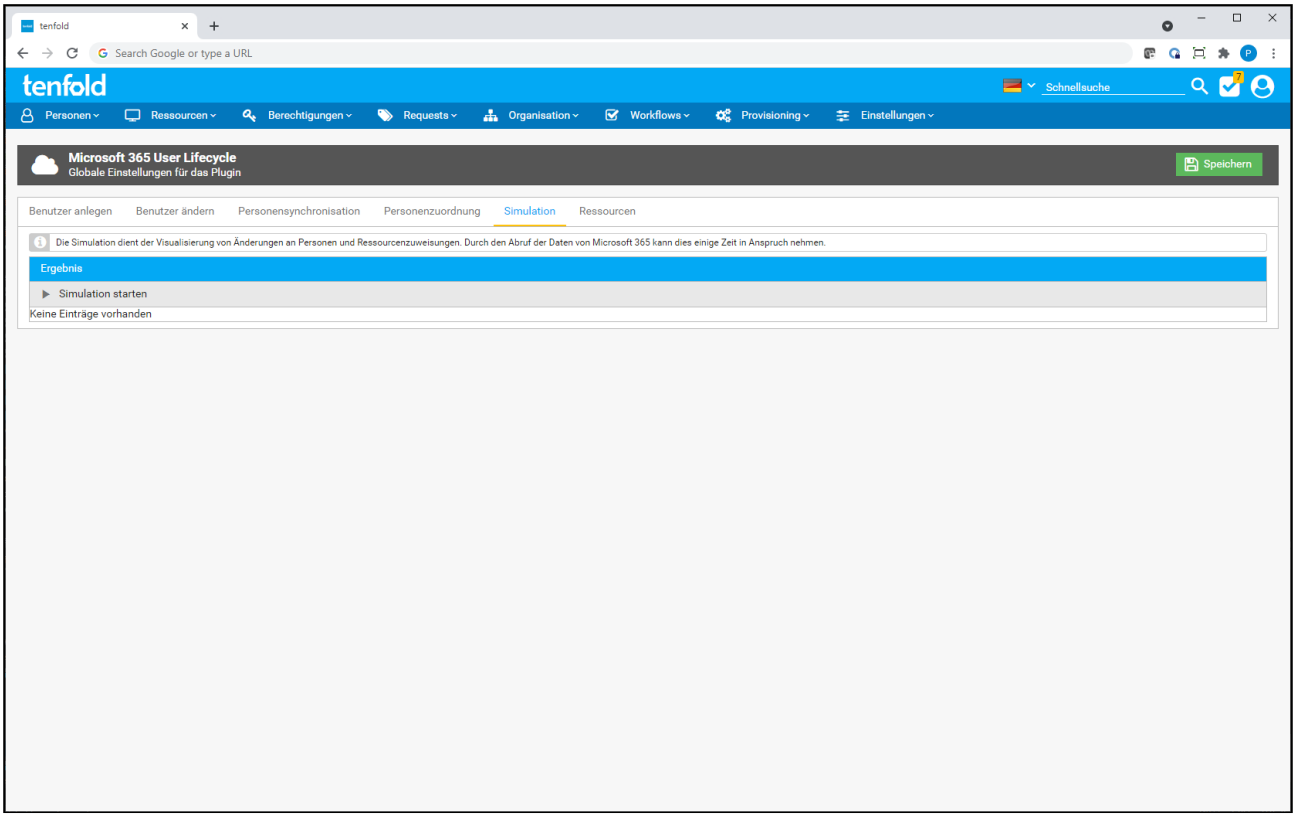
**==**

Verwenden Sie für Vergleiche immer den Operator "==". Bei dem Operator "=" handelt es sich um eine Zuweisung von Werten.

**Speichern**

Sie können die Einstellungen des Plugins erst speichern, wenn Sie mindestens eine Regel eingetragen haben.

## Simulation

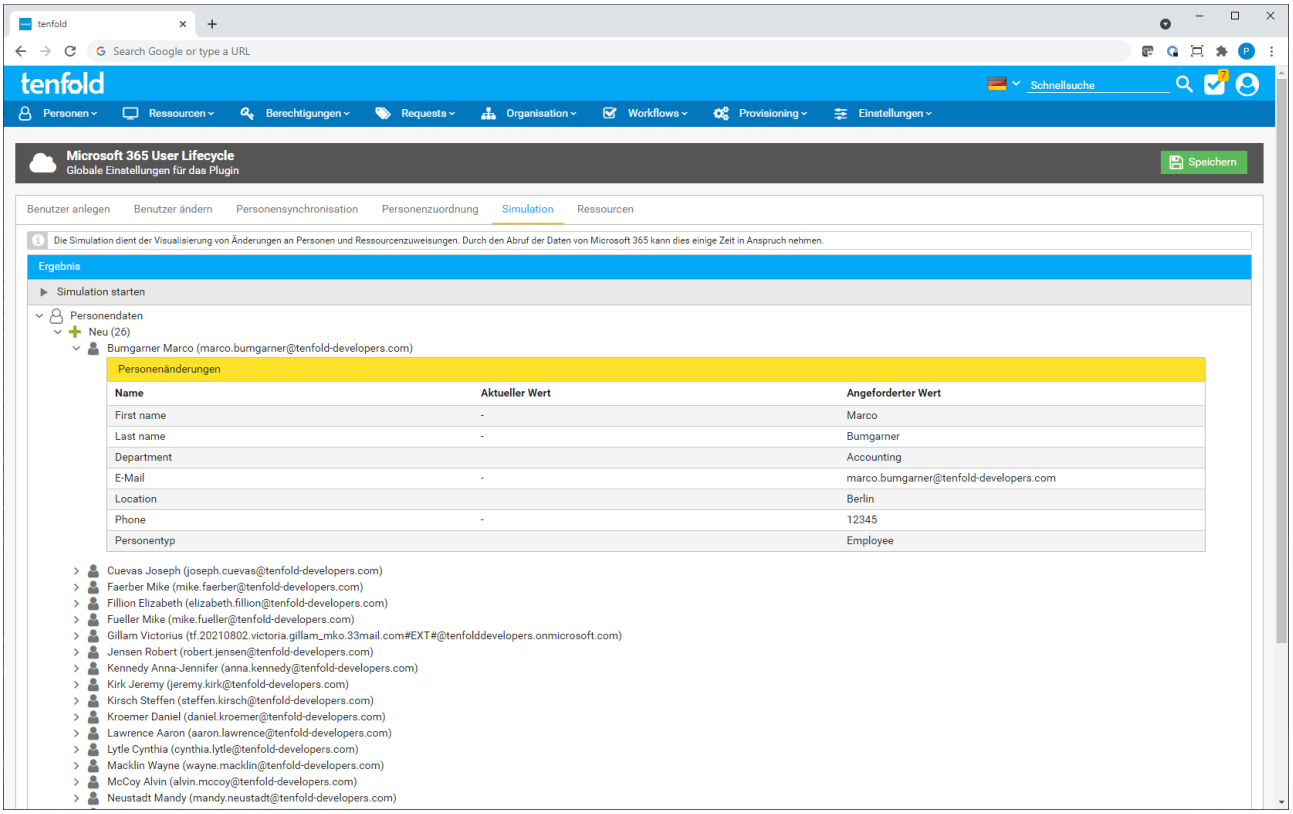



Auf diesem Karteireiter können Sie eine Simulation des Imports durchführen lassen. Zum Starten der Simulation klicken Sie auf die Schaltfläche "Simulation starten".

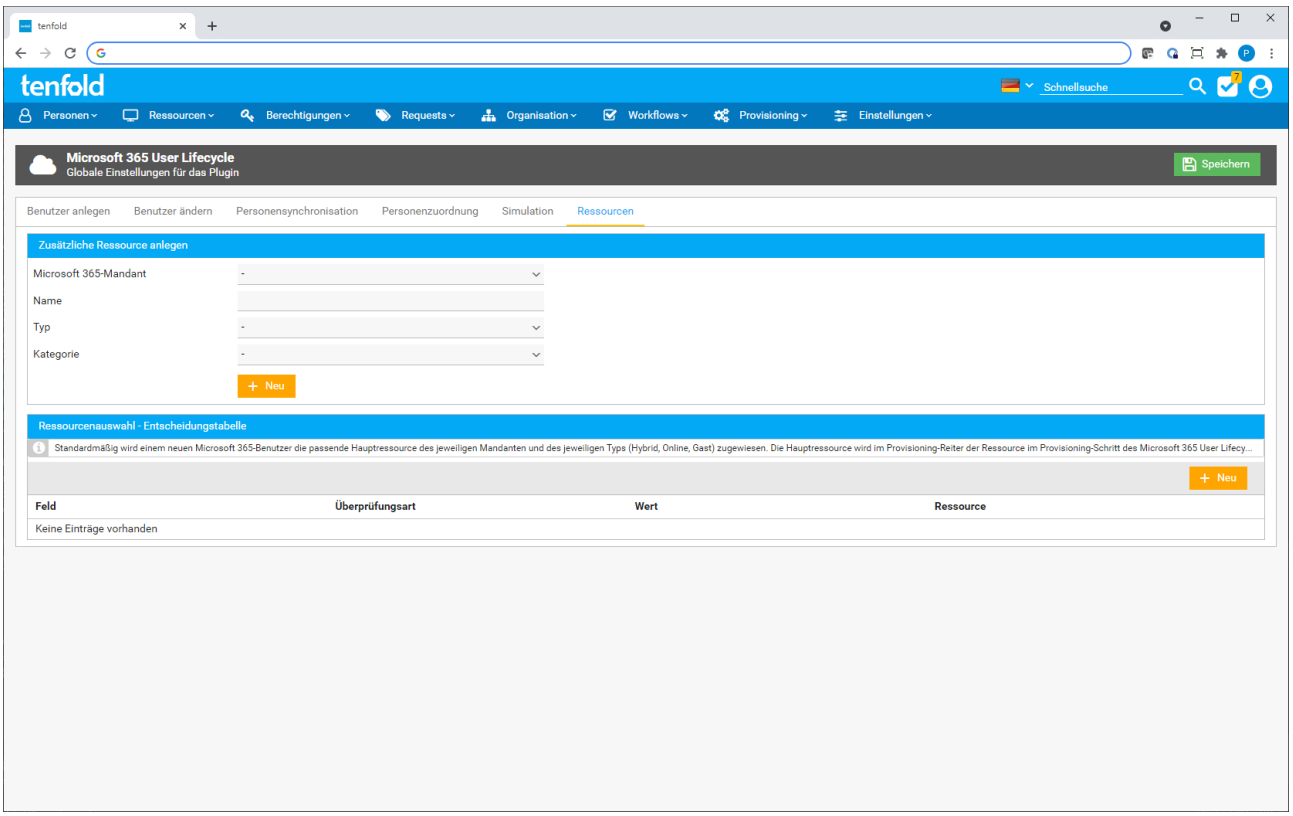
**Dauer**

Da alle Benutzer aus Ihren Microsoft 365-Mandanten ausgelesen werden kann dieser Vorgang einige Zeit in Anspruch nehmen.

Nachdem die Simulation abgeschlossen ist, erhalten Sie eine Übersicht über sämtliche Änderungen, die der Import durchführen würde. An dieser Stelle werden in keinem Fall Änderungen vorgenommen.


tenfold
Search Google or type a URL
Schnellsuche
Personen
Ressourcen
Berechtigungen
Requests
Organisation
Workflows
Provisioning
Einstellungen
Microsoft 365 User Lifecycle
Globale Einstellungen für das Plugin
Speichern
Benutzer anlegen
Benutzer ändern
Personensynchronisation
Personenzuordnung
Simulation
Ressourcen
Die Simulation dient der Visualisierung von Änderungen an Personen und Ressourcenzuweisungen. Durch den Abruf der Daten von Microsoft 365 kann dies einige Zeit in Anspruch nehmen.
Ergebnis
Simulation starten
Personendaten
Neu (26)
Bumgarner Marco (marco.bumgarner@tenfold-developers.com)
Personenänderungen
Name
Aktueller Wert
Angeforderter Wert
First name - Marco
Last name - Bumgarner
Department - Accounting
E-Mail - marco.bumgarner@tenfold-developers.com
Location - Berlin
Phone - 12345
Personentyp - Employee
Cuevas Joseph (joseph.cuevas@tenfold-developers.com)
Faerber Mike (mike.faerber@tenfold-developers.com)
Fillion Elizabeth (elizabeth.fillion@tenfold-developers.com)
Fueller Mike (mike.fueller@tenfold-developers.com)
Gillam Victorius (tf.20210802.victoria.gillam_mko.33mail.com#EXT#@tenfolddevelopers.onmicrosoft.com)
Jensen Robert (robert.jensen@tenfold-developers.com)
Kennedy Anna-Jennifer (anna.kennedy@tenfold-developers.com)
Kirk Jeremy (jeremy.kirk@tenfold-developers.com)
Kirsch Steffen (steffen.kirsch@tenfold-developers.com)
Kroemer Daniel (daniel.kroemer@tenfold-developers.com)
Lawrence Aaron (aaron.lawrence@tenfold-developers.com)
Lytle Cynthia (cynthia.lytle@tenfold-developers.com)
Macklin Wayne (wayne.macklin@tenfold-developers.com)
McCoy Alvin (alvin.mccoy@tenfold-developers.com)
Neustadt Mandy (mandy.neustadt@tenfold-developers.com)

## Ressourcen


tenfold
Schnellsuche
Personen
Ressourcen
Berechtigungen
Requests
Organisation
Workflows
Provisioning
Einstellungen
Microsoft 365 User Lifecycle
Globale Einstellungen für das Plugin
Speichern
Benutzer anlegen
Benutzer ändern
Personensynchronisation
Personenzuordnung
Simulation
Ressourcen
Zusätzliche Ressource anlegen
Microsoft 365-Mandant
Name
Typ
Kategorie
Neu
Ressourcenauswahl - Entscheidungstabelle
Standardmäßig wird einem neuen Microsoft 365-Benutzer die passende Hauptressource des jeweiligen Mandanten und des jeweiligen Typs (Hybrid, Online, Gast) zugewiesen. Die Hauptressource wird im Provisioning-Reiter der Ressource im Provisioning-Schritt des Microsoft 365 User Lifecy...
Neu
Feld
Überprüfungsart
Wert
Ressource
Keine Einträge vorhanden

Auf diesem Karteireiter können Sie neue Ressourcen anlegen, welche Microsoft 365-Benutzerkonten darstellen.

> **Essentials 365**
>
> Sie können mit dieser Funktion auch Ressourcen anlegen, wenn Sie die Essentials 365 Version von tenfold Lizenziert haben, die das Anlegen neuer Ressourcen sonst eigentlich nicht gestattet.

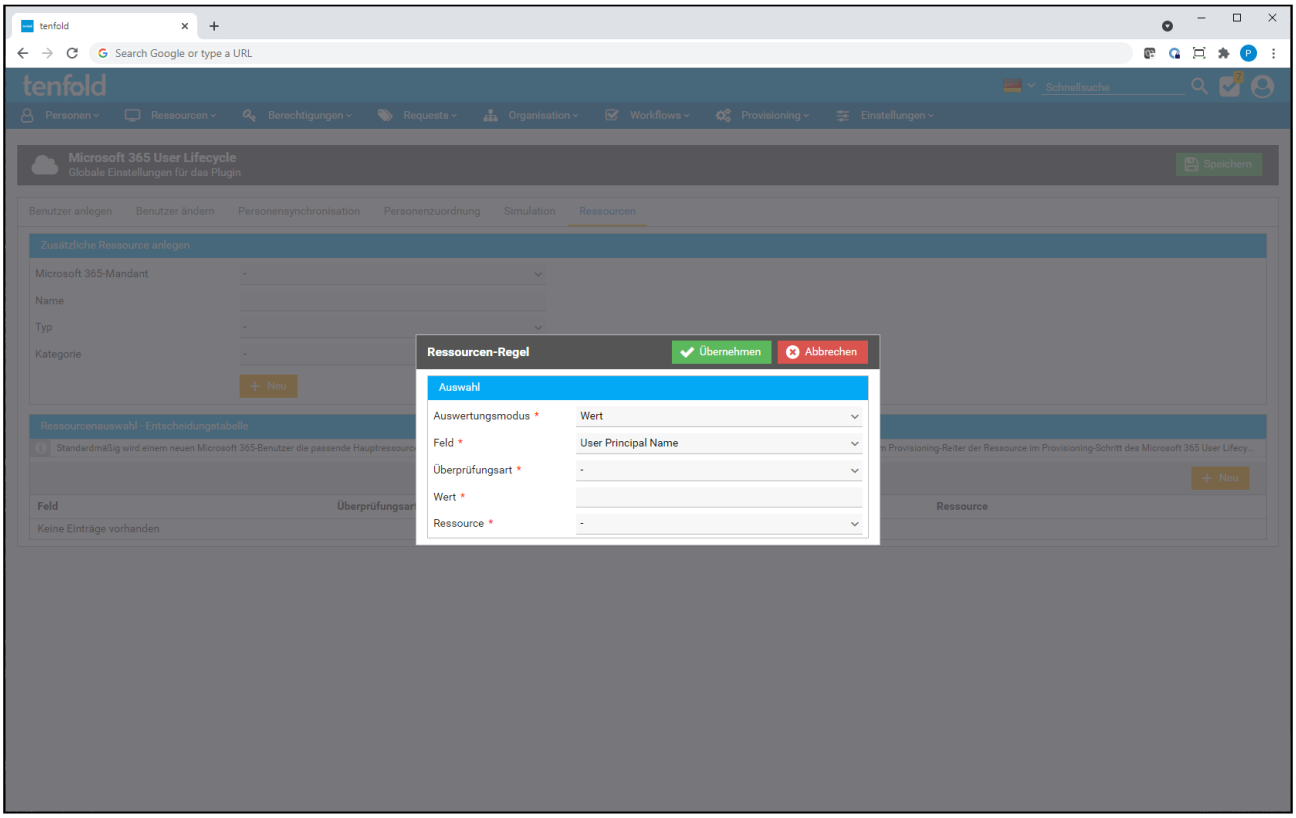
Zum Anlegen einer neuen Ressource treffen Sie folgende Einstellungen und betätigen die Schaltfläche "Neu".

| Einstellung | Beschreibung |
|---|---|
| Microsoft 365-Mandant | Wählen Sie hier den Mandanten aus, für den die Ressource angelegt werden soll. |
| Name | Der Name, mit welchem die Ressource angelegt werden soll. |
| Typ | Hier stellen Sie den Typ von Benutzerkonto ein, welcher durch die Ressource verwaltet wird. Sie können hier "Hybrid", "Online" oder "Gast" auswählen. |
| Kategorie | Sollten Sie einer Person mehrere Konten desselben Typs zuordnen wollen, müssen Sie hier eine Kategorie auswählen, um zu unterscheiden, welchem Zweck das Konto dient.<br>**Beispiel:** Sie möchten für eine Person sowohl ein normales Benutzerkonto als auch ein Administratorkonto einrichten, daher legen Sie zwei Ressourcen an: eine der Kategorie "User" und eine der Kategorie "Administrator". In Profilen können Sie daraufhin unterscheiden, welcher Kontokategorie welche Microsoft 365-Gruppen zugeordnet werden (siehe Profile(see page 168)). |

Bei der Zuordnung von Ressourcen durch den Import weist tenfold einer Person immer die Hauptressource des entsprechenden Typs (Online, Hybrid oder Gast) und Mandanten zu.

> **Hauptressource**
>
> Eine Ressource können Sie im Provisioning des Microsoft 365 User Lifecycle Plugin Provisionierungschrittes der entsprechenden Ressource als Hauptressource markieren. Gehen Sie hierfür auf die Maske Ressourcen > Verwaltung, bearbeiten die gewünschte Ressource und klicken dort im Provisionierungsschritt des Microsoft 365 User Lifecycle Plugins auf die Schaltfläche "Hauptressource".

Sollten Sie mehrere Ressourcen für einen Mandanten und Typen definiert haben, müssen Sie für sämtliche Ressourcen, welche nicht Hauptressourcen sind, eine Regel anlegen, damit tenfold diese beim Import erkennen kann.
Um eine neue Regel anzulegen, klicken Sie auf die Schaltfläche "Neu". Es öffnet sich daraufhin ein Dialog, in welchem Sie die Regel definieren können.




Folgende Einstellungen stehen zur Verfügung:

| Einstellung | Beschreibung |
|---|---|
| Auswertungsmodus | Legen Sie hier fest, ob die Regel durch einen Wertevergleich oder ein Code Snippet ausgewertet werden soll. |
| Feld | Legen Sie hier das zu vergleichende Feld fest. Diese Einstellung ist nur sichtbar, wenn Sie in der Einstellung "Auswertungsmodus" die Auswahl "Feld" getroffen haben. |
| Überprüfungsart | Hier können Sie einstellen wie das ausgewählte Feld verglichen werden soll. Diese Einstellung ist nur sichtbar, wenn in der Einstellung "Feld" ein Feld ausgewählt wurde.<br>Folgende Auswahlmöglichkeiten stehen Ihnen zur Verfügung:<br>• **Beginnt mit:** Das Feld muss mit dem angegebenen Wert beginnen.<br>• **Endet mit:** Das Feld muss mit dem angegebenen Wert enden.<br>• **Enthält:** Der angegebene Wert muss irgendwo in dem Feld vorkommen.<br>• **Ist gleich:** Der angegebene Wert muss dem Feld zur Gänze entsprechen. |
| Wert | Mit dieser Einstellung wird der Wert bestimmt, mit welchem das Feld in der angegebenen Überprüfungsart verglichen wird. |

| Einstellung | Beschreibung |
| --- | --- |
| Code Snippet | Mit diesem Code Snippet kann geprüft werden, ob die ausgewählte Ressource der Regel verwendet werden soll. Sie erhalten die Variable "user", mit welcher Sie auf die Daten eines Kontos zugreifen können (Beispiel: "user.givenName" für den Vornamen). Es muss der Wert "true" zurückgeliefert werden, damit diese Regel als erfüllt gilt. |
| Ressource | Die Ressource, welche zugewiesen werden soll, wenn diese Regel als erfüllt gilt. |

Für jedes Konto in Microsoft 365 werden alle hier eingestellten Regeln durchgeführt. Die eingestellte Ressource der Regel, die als erste zutrifft, wird der Person zugeordnet, welche durch die Personenzuordnung ermittelt wurde.

> **Reihenfolge**
>
> Sie können die Reihenfolge der Regeln mittels Drag & Drop verändern.

# 15 Sicherheit und Datenschutz

## 15.1 Datenschutzhinweise

### 15.1.1 Zweck der Anwendung

Die Anwendung "tenfold" dient der Verwaltung und dem Reporting im Zusammenhang mit den IT-Zugriffsberechtigungen in Organisationen. Zu den Aufgaben, für die tenfold eingesetzt werden kann, gehören inbesondere folgende:

- Anlage von Benutzerkonten in IT-Systemen (in Active Directory und bei Bedarf auch in anderen Anwendungen)
- Deaktivierung von nicht mehr benötigten Benutzerkonten
- Zuordnung und Entzug von IT-Zugriffsberechtigungen auf unterschiedlichen Systemen (Fileservern, Mailsystemen, diversen Anwendungen)

### 15.1.2 Arten der verarbeiteten Daten

Nachfolgende Daten, welche eine Relevanz zum Datenschutz haben können, werden in tenfold verarbeitet. Für alle Datenarten gilt, dass diese sowohl die aktuelle Situation erfassen, als auch alle historischen Daten, die seit der initialen Installation von tenfold aufgezeichnet wurden. Es erfolgt keine automatische Lösung von Altdaten.

#### Benutzerstammdaten

Es werden für alle Mitarbeiter, die in tenfold erfasst werden, bestimmte personenbezogene Attribute erfasst. Üblicherweise sind dies: Vorname, Nachname, Abteilung, Standort, Kostenstelle, Personalnummer, berufliche Kontaktinformationen. Insbesondere für die in Artikel 9 DSGVO aufgezählten Datenkategorien sind keine entsprechenden Strukturen vorgesehen.

### Berechtigungsdaten

Daten über die IT-Berechtigungen der Mitarbeiter werden verarbeitet. Die Informationen stellen dar, auf welche Ressourcen ein Mitarbeiter zugreifen kann (beispielweise, ob der Zugriff auf ein bestimmtes Verzeichnis auf einer Freigabe erlaubt ist, oder nicht). Nicht verarbeitet werden hingegen die tatsächlich genutzten Zugriffe. Insofern wird nicht dokumentiert, welcher Mitarbeiter wann auf welche Daten tatsächlich zugegriffen hat.

### Antragsdaten

Alle Details zu im System erfassten Anträgen werden dokumentiert. Dies umfasst den Antragsteller, den Zeitpunkt der Antragstellung, alle Details zu etwaigen Genehmigungen aus Workflows (Genehmiger, Zeitpunkt der Genehmigung, ggf. Kommentare), Details zu den zu manipulierenden Ressourcen, alle Datenmanipulation, die über die entsprechende Schnittstelle im Zielsystem stattgefunden haben und aufgetretene Verarbeitungsfehler.

### Systemeinstellungen

Systemeinstellungen und Konfigurationseinstellungen werden gespeichert. Bei ausgewählten Einstellungen wird gespeichert, welche Person diese angelegt, zuletzt bearbeitet, beziehungsweise gelöscht hat. Systemeinstellungen werden, bis auf wenige Ausnahmen, nicht historisiert gespeichert.

## 15.1.3 Verfahren zur Datenverarbeitung

Alle Daten werden in der tenfold Datenbank gespeichert. Der Zugriff auf diese Datenbank muss gegen unberechtigten Zugriff geschützt werden. Lediglich das tenfold Dienstkonto sowie der Datenbankadministrator sollten auf die Datenbank Zugriff haben.

## 15.1.4 Zugriffskontrollen

Über entsprechende Zugriffskontrollen kann insbesondere gesteuert werden:

- Berechtigung zur Antragstellung für die Zuordnung / für den Entzug von Ressourcen für bestimmte Personenkreise (Abteilungen, Standorte, etc.)
- Verantwortlichkeiten für bestimmte Ressourcen, und damit einhergehend die Möglichkeit Anträge auf Zugriff auf die betreffende Ressource freizuschalten
- Berechtigung zur Anzeige von Berechtigungsdaten beziehungsweise die Berechtigung, Berichte zu generieren
- Berechtigung zur Veränderung der tenfold-Konfiguration

Diese Berechtigungen können granular, und in vielen Fällen abhängig zur Organisationseinheit, eingestellt werden. IT-Administratoren sollten von der Verantwortlichkeit für Ressourcen ausgeschlossen werden, damit die Entscheidung über Berechtigungsfreigaben tatsächlich beim Datenverantwortlichen der jeweiligen Ressource liegt. Die Zuordnung erfolgt in tenfold über Berechtigungsrollen. Für die Zuordnung der Berechtigungsrollen ist der IT-Administrator verantwortlich.

# 15.2 Datenschutzrichtlinie

Gemäß der EU-Datenschutz-Grundverordnung (EU-DSGVO) Artikel 5(1)e, dürfen Unternehmen die Daten, welche eine Person identifizieren können nicht für immer aufbewahren.

1. *Personenbezogene daten müssen*

...

*e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß* Artikel 89 Absatz 1[13] *verarbeitet werden ("**Speicherbegrenzung**");* { *Auszug von* https://www.datenschutz-grundverordnung.eu/grundverordnung/art-5-ds-gvo/ *Stand 28.11.2022* }

**Wie lange dürfen/müssen Daten aufbewahrt werden?**

Erkennbar ist hierbei, dass die EU-DSGVO keine festgelegten Zeitrahmen vorgibt, nach welchen Zeiträumen die Daten entfernt werden müssen. Dies liegt daran, dass es für unterschiedliche Unternehmen und Branchen unterschiedliche Richtlinien gibt, wie lange Daten eventuell sogar aufbewahrt werden müssen. Banken und Versicherungen haben beispielsweise andere Vorgaben als Produktionsbetriebe.

Um diesen unterschiedlichen Vorgaben gerecht werden zu können, bietet tenfold die Möglichkeit flexible Zeiträume zur automatischen Anonymisierung/Löschung historischer Daten zu konfigurieren.

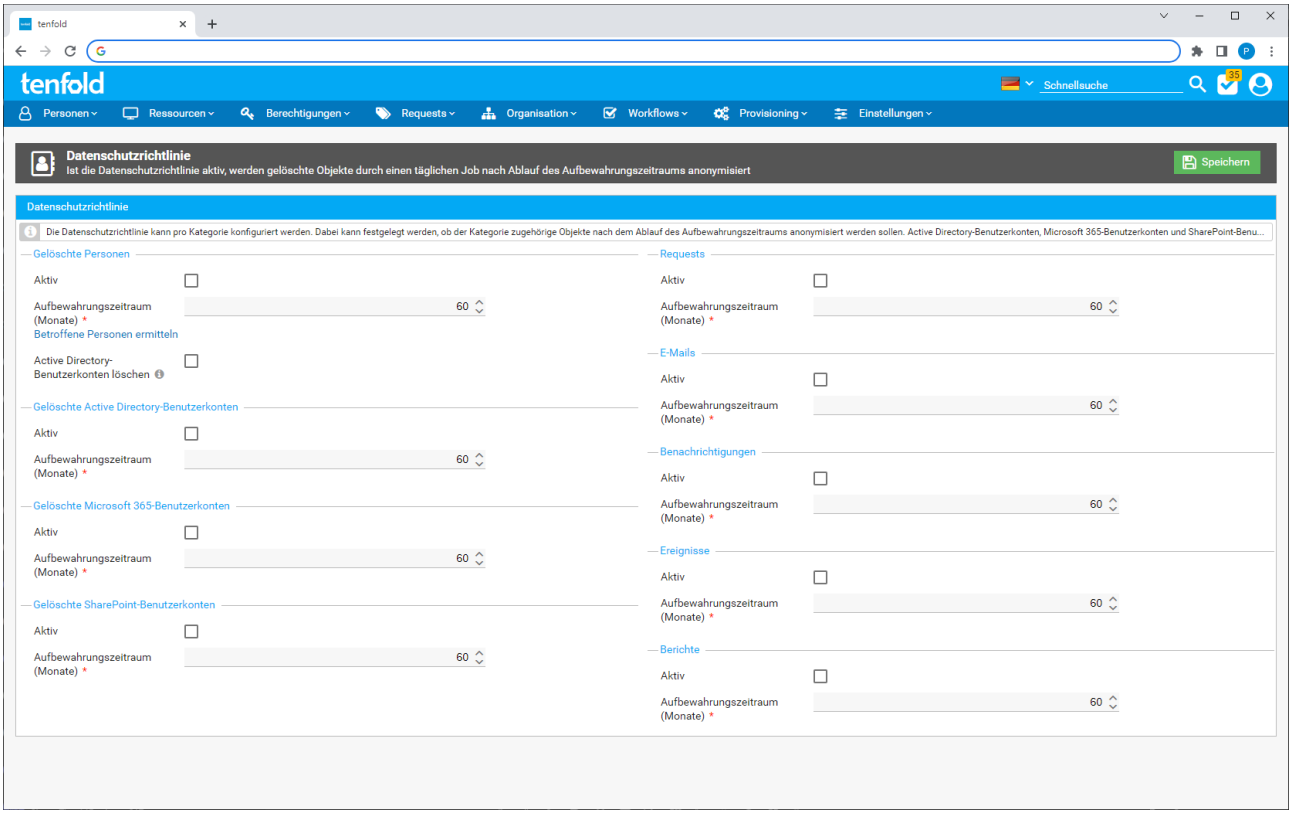
## 15.2.1 Richtlinie verwalten

Zur Verwaltung der Datenschutzrichtlinie navigieren Sie im Menü zu Einstellungen > Richtlinien > Datenschutzrichtlinie.

**Benötigte Berechtigung**

Für die Verwaltung wird die Berechtigung "Manage Privacy Policy" (9250) benötigt.

13 https://www.datenschutz-grundverordnung.eu/grundverordnung/art-89-ds-gvo/




Auf dieser Maske können Sie festlegen, wie lange bestimmte Daten aufgehoben werden, bevor diese anonymisiert oder endgültig gelöscht werden.

> **Warum anonymisieren?**
>
> Durch die Historisierung der Daten in tenfold ist es in den meisten Fällen nicht möglich die Daten komplett aus der Datenbank zu löschen, da diese in Beziehungen zu anderen Datensätzen stehen (welche möglicherweise sogar noch aktiv sind). Stattdessen werden in diesen Datensätzen die notwendigen Spalten geleert und die Datensätze als "anonymisiert" markiert.

Sie können hier für verschiedene Objektarten definieren, ob die automatische Anonymisierung aktiv ist, und wie lange der Aufbewahrungszeitraum für diese Objekte ist.

Hierbei zu beachten ist, dass es von den Objekten abhängt, wann der Zeitraum zu laufen beginnt.

| Objekt | Beginn des Aufbewahrungszeitraums |
|---|---|
| Gelöschte Personen | Der Zeitraum beginnt mit dem Zeitpunkt an dem die Person gelöscht wurde. Historische Datensätze zu aktiven Personen werden nicht anonymisiert, bevor die Person gelöscht wurde. |
| Gelöschte Active Directory-Benutzerkonten | Der Zeitraum beginnt mit dem Zeitpunkt an dem das Objekt gelöscht wurde. Historische Datensätze zu aktiven Active Directory-Objekten werden nicht automatisch anonymisiert, bevor das Objekt gelöscht wurde. **Achtung:** Dies betrifft nur Active Directory-Objekte, welche keiner Person zugeordnet wurden. Konten welche zu einer Person gehören, werden mit der Person gemeinsam anonymisiert und von dieser Einstellung nicht beachtet. |

| Objekt | Beginn des Aufbewahrungszeitraums |
|---|---|
| Gelöschte Microsoft 365-Benutzerkonten | Der Zeitraum beginnt mit dem Zeitpunkt an dem das Objekt gelöscht wurde. Historische Datensätze zu aktiven Microsoft 365-Objekten werden nicht automatisch anonymisiert, bevor das Objekt gelöscht wurde. **Achtung:** Dies betrifft nur Microsoft 365-Objekte, welche keiner Person und keinem Active Directory-Objekt zugeordnet wurden. Objekte welche zu einer Person oder Active Directory-Objekt gehören, werden mit den jeweiligen Datensätzen gemeinsam anonymisiert und von dieser Einstellung nicht beachtet. |
| Gelöschte SharePoint-Benutzerkonten | Der Zeitraum beginnt mit dem Zeitpunkt an dem das Konto gelöscht wurde. Historische Datensätze zu aktiven SharePoint-Konten werden nicht anonymisiert bevor das Objekt gelöscht wurde. **Hinweis:** Hierbei handelt es sich um die (historischen) Daten von SharePoint-Benutzerkonten. Diese können zu einem Microsoft 365-Mandaten oder einer On Premises-Installation von SharePoint gehören. |
| Requests | Der Zeitraum beginnt mit der Anlage des Requests. Requests werden automatisch anonymisiert unabhängig davon ob die betroffene Person oder das betroffene Objekt aktiv sind oder nicht. |
| E-Mails | Der Zeitraum beginnt mit dem Versand der E-Mail. Hierbei wird nur der Eintrag in der E-Mail-Historie von tenfold (siehe Historie gesendeter E-Mails(see page 536)) anonymisiert. Die E-Mails welche in den Postfächern liegen, sind davon nicht betroffen. |
| Benachrichtigungen | Der Zeitraum beginnt mit der Erstellung der Benachrichtigung. Hierbei wird nur der Benachrichtigungsdatensatz in tenfold anonymisiert. Die Nachrichten welche dadurch in Fremdsystemen erzeugt wurden (z.B. Tickets oder E-Mails) sind davon unbetroffen und müssen in den jeweiligen Systemen selbst entfernt werden. |
| Ereignisse | Der Zeitraum beginnt mit der Erstellung des Ereignisses. **Achtung:** Ereignisse, welche zu Requests gehören, werden mit der Anonymisierung von Ereignissen **nicht** anonymisiert, stattdessen werden sie gemeinsam mit den Requests anonymisiert. |
| Berichte | Der Zeitraum beginnt mit der Erstellung des Berichts. Berichte werden unabhängig davon anonymisiert, ob die Person oder das Objekt, zu welchem der Bericht gemacht wurde, noch aktiv ist oder nicht. |

Für Personen lässt sich darüber hinaus noch einstellen, ob dazugehörige Active Directory-Objekte bei der Anonymisierung gelöscht werden sollen. Ist diese Einstellung nicht aktiv, werden nur in der tenfold-Datenbank die Daten anonymisiert, das Active Directory-Konto der Person bleibt jedoch mit allen Daten bestehen und muss manuell entfernt werden.

## 15.2.2 Manuelle Anonymisierung

Die EU-DSGVO sieht auch vor, dass eine Person verlangen kann, dass Daten umgehend zu löschen sind. Um diesen Forderungen nachgehen zu können, lassen sich Personendatensätze manuell sofort anonymisieren.

**Benötigte Berechtigung**

Für die manuelle Anonymisierung ist die Berechtigung "Anonymize Person" (9251) erforderlich.

Verwenden Sie hierfür die Schnellsuche um nach der betroffenen Person zu suchen und wählen im Aktionsmenü der Person die Aktion "Anonymisieren" aus.

**Gelöschte Personen**

Die manuelle Anonymisierung von Personen ist nur für Personen möglich, welche als gelöscht markiert wurden. Dies ist standardmäßig für Personen der Fall, welche sich in der Lifecycle-Phase "Gelöscht" befinden. Um diese Personen zu finden, stellen Sie sicher, dass die Option "Gelöschte Personen und unvollständige Personenanlagen" bei der Schnellsuche aktiviert wurde.

Nachdem Sie die Aktion ausgewählt haben, wird Ihnen ein Dialog angezeigt, welcher die zu der Person gehörenden Objekte anzeigt. Darunter finden Sie den Personenstammdatensatz aus tenfold und etwaige Active Directory- oder Microsoft 365-Objekte. Sollte es unter den Active Directory- und Microsoft 365-Objekten noch aktive Konten geben, erhalten Sie einen Warnhinweis in der Zeile des jeweiligen Objektes. Betätigen Sie die Schaltfläche "Anonymisieren" um die Anonymisierung durchzuführen. Es werden daraufhin alle Schritte durchgeführt, wie sie in der Datenschutzrichtlinie für Personen hinterlegt sind, welche bei der automatisierten Anonymisierung durchgeführt werden. Die Zeiträume sind hierbei in Monaten anzugeben.

## 15.2.3 Welche Daten werden anonymisiert?

Je nachdem welche Daten anonymisiert werden, werden die relevanten Spalten folgender Tabellen anonymisiert.

| Anonymisiertes Objekt | Tabelle |
|---|---|
| **Gelöschte Person** | **PERSON** |
| | PERSON_MASTERDATA |
| | EX_OUT_OF_OFFICE |
| | SOD_VIOLATION |
| | SOD_VIOLATION_DATA |
| | PERSON_PICTURE |
| | PERSON_VERF_QUESTION |
| | SERVICE_ASSIGNMENT |
| | PERSON_DOCUMENT |
| | PERSON_DOCUMENT_DATA |
| | Alle Tabellen aus den Bereichen für gelöschte Active Directory- und Microsoft 365-Objekten. |

| | |
|---|---|
| **Gelöschtes Active Directory-Objekt** | **ADS_OBJECT** (Ausgangspunkt der Anonymisierung, enthält jedoch selbst keine Daten die anonymisiert werden) |
| | ADS_OBJECT_DATA |
| | EX_MAILBOX_DATA |
| | EX_OUT_OF_OFFICE |
| | SP_OBJECT_DATA |
| **Gelöschtes Microsoft 365-Objekt** | **O365_OBJECT** (Ausgangspunkt der Anonymisierung, enthält jedoch selbst keine Daten die anonymisiert werden) |
| | O365_OBJECT_DATA |
| | EX_MAILBOX_DATA |
| | EX_OUT_OF_OFFICE |
| **Gelöschtes SharePoint-Konto** | **SP_OBJECT** (Ausgangspunkt der Anonymisierung, enthält jedoch selbst keine Daten die anonymisiert werden) |
| | SP_OBJECT_DATA |
| **Request** | **REQUEST** |
| | REQUEST_ATTACHMENT |
| | REQUEST_ERROR |
| | SCRIPT_LOG_ERROR |
| | EVENT |
| **Ereignis** | **EVENT** |
| **E-Mail** | **NOTIFICATION_LOG** |
| | NOTIFICATION_LOG_ERROR |
| **Benachrichtigung** | **ALERT** |
| **Bericht** | **RPT_00_* (Alle Tabellen die mit RPG_00 beginnen)** |
| | **RPT_01_* (Alle Tabellen die mit RPT_01 beginnen)** |

Ausgehend vom Objekt welches anonymisiert wird (fettgedruckt in der Tabelle oberhalb), werden alle notwendigen Daten in den verknüpften Tabellen anonymisiert. Hierbei werden die personenbezogenen Daten durch "-" ersetzt. Die Ausgangsobjekte selbst, werden ebenso als "anonymisiert" markiert. Die Markierung der

Objekte hat den Zweck, dass diese von diversen Scans (siehe Jobs(see page 443)) nicht mehr eingelesen werden, sollten die Daten in den Fremdsystemen noch vorhanden sein.

## 15.3 Hinweise zu Betroffenenrechten laut DSGVO

### 15.3.1 Grundsätzliches

Personenbezogene Daten werden, abhängig von der Systemkonfiguration, für Mitarbeiter sowie externe Personen (z.B. Lieferanten oder Kunden) in tenfold gespeichert. Welche Kategorien von Daten konkret gespeichert werden, ist von der Systemkonfiguration, im speziellen der eingestellten Personenfelder, abhängig.

### 15.3.2 Recht auf Auskunft (Art. 15 DSGVO)

Personenbezogene Daten werden in entsprechenden Personenfeldern des zugehörigen Stammdatensatzes gespeichert. Eine Datenauskunft kann durch Kopie des entsprechenden Datensatzes über Bildschirmfoto erstellt werden. Darüber hinaus ist zu beachten:

- Der Zweck der Verarbeitung ist dabei die Steuerung von IT-Benutzerkonten und IT-Zugriffsrechten durch eine Identity & Access Management Lösung.
- Die Kategorien der Daten, die verarbeitet werden, ergeben sich aus den konfigurierten Personenfeldern
- Die geplante Speicherdauer beträgt zumindest die Dauer des Vertragsverhältnisses (Dienstvertrag, Werkvertrag, etc.)
- Ein Widerspruchsrecht gegen die Verarbeitung besteht in der Regel nicht
- Die Herkunft der Daten ist abhängig von der Konfiguration der Personenfelder, liegt aber für gewöhnlich beim Unternehmen selbst
- Ob weitere Empfänger oder Kategorien von Empfängern existieren, muss im Einzelfall bewertet werden

### 15.3.3 Recht auf Berichtigung (Art. 16 DSGVO)

Das Recht von Betroffenen auf Berichtigung kann über die Korrektur oder Vervollständigung der Daten innerhalb der konfigurierten Personenfelder berücksichtigt werden.

### 15.3.4 Recht auf Löschung (Art. 17 DSGVO)

Das Recht auf Löschung besagt, dass Daten, für die ein Verantwortlicher keine Rechtsgrundlage zur Datenverarbeitung mehr hat, gelöscht werden müssen. Im Kontext dieser Software tritt dies üblicherweise dann ein, wenn die Aufbewahrungsfristen für vertragliche Daten abgelaufen sind. Eine tatsächliche Löschung der personenbezogenen Daten ist aufgrund von technischen Umständen (Konsistenzen in der Datenbank) nicht möglich. Es wird daher in der Software eine Funktion angeboten, welche es ermöglicht, personenbezogene Daten vollständig zu anonymisieren. Dabei sind zwei Varianten vorgesehen:

- Anonymisierung der Daten einer spezifischen Person
- Anonymisierung der Daten aller Personen, bei denen die Grundlage für die Verarbeitung seit einem festzulegenden Zeitraum entfallen ist

### 15.3.5 Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

Der Zweck des Rechts auf Datenübertragbarkeit liegt vordergründig darin, dass Betroffenen durch die Übertragung ihrer Daten von einem Verarbeiter (Anbieter) zu einem anderen beispielweise Anbieterwechsel einfacher ermöglicht werden. Eine Übertragung der in dieser Software verarbeiteten Daten von einem Arbeitgeber oder Vertragspartner zu einem anderen ist üblicherweise nicht zweckmäßig und auch dem

Verbraucherschutz nicht zuträglich. Das Recht auf (automatische) Datenübertragbarkeit ist daher bis auf weiteres nicht abgebildet.

### 15.3.6 Recht auf Widerspruch (Art. 21 DSGVO)

Nachdem die Verarbeitung der Daten nicht aufgrund Art. 6 Abs. 1 Buchstabe e oder f erfolgt, besteht kein Recht auf Widerspruch.

## 15.4 Technische Sicherheitsinformationen

> **Achtung**
>
> Diese Sicherheitsinformationen sind für den Betrieb von tenfold zwingend zu beachten. Wenn die Richtlinien und Empfehlungen nicht zur Gänze berücksichtigt und umgesetzt werden, kann keine Gewährleistung für den sicheren Betrieb gegeben werden.

### 15.4.1 Allgemeine Hinweise

Folgende allgemeine Sicherheitshinweise gelten grundlegend:

- Stellen Sie sicher, dass der/die Server, auf denen Sie tenfold betreiben immer alle aktuellen Sicherheitsupdates enthält
- Darüber hinaus ist sicherzustellen, dass auf dem tenfold Application Server immer das aktuelle Update der jeweiligen unterstützten Java Major Version installiert wurde.
- Das gleiche gilt für die jeweilige .NET Version für alle Server, auf denen ein tenfold Agent installiert ist
- Stellen Sie darüber hinaus sicher, dass dies auch für den Datenbankserver, sowie für alle Server auf denen ein tenfold Agent betrieben wird, gilt.
- Wenn an einem beliebigen Punkt Passworte gewählt werden müssen (z.B. für die Zugangsdaten zur tenfold Datenbank) , dann stellen Sie sicher, dass diese den Empfehlungen des BSI entsprechen (Siehe https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2011/Passwortsicherheit_27012011.html).

### 15.4.2 Datenbanksicherheit

#### Zugang zur Datenbank

tenfold speichert alle Einstellungen, Benutzer- und Berechtigungsdaten sowie andere Bewegungsdaten in einer SQL-Datenbank. Unterstützt werden die Systeme Microsoft SQL Server, Oracle Database und MySQL. Für alle Datenbanken gilt:

- Die Zugriffsrechte für den Verbindungsbenutzer für tenfold müssen Lesen und Schreiben auf alle Objekte in der Datenbank erlauben
- Die Zugriffsrechte des IT-Administrators sollten auf lesenden Zugriff beschränkt werden
- Alle anderen Benutzer sollten keine Rechte haben, sich zur Datenbank zu verbinden oder irgendwelche Objekte darin zu lesen

Um die Authentifizierung bei der Datenbank durchführen zu können, gibt es zwei Möglichkeiten: Integrierte Windows-Authentifizierung für Microsoft SQL Server oder Authentifizierung per Benutzername und Passwort (für Oracle und MySQL steht nur diese Option zur Verfügung). Im Falle der Authentifizierung per Benutzername und Passwort sind die Zugangsdaten in einer Konfigurationsdatei gespeichert. Der Zugriff auf diese Datei muss entsprechend abgesichert werden (siehe unten).

### Passworte für Fremdsysteme

tenfold benötigt zur Arbeit in Fremdsystemen ein entsprechend berechtigtes Konto in dem jeweiligen Fremdsystem. Beispielweise können dies folgende sein:

- Active Directory: Dienstkonto zum Ändern von Benutzerkonten, Anlegen von Gruppen, etc.
- SQL-Datenbank: Dienstkonto, um DML-Statements auf der Datenbank ausführen zu können
- SAP: RFC-User für Funktionsaufrufe im SAP

Die Zugangsdaten für diese Benutzer sind in der Datenbank in der Tabelle CREDENTIALS, Spalte PASSWORD gespeichert. Die Daten werden über das asynchrone Verschlüsselungsverfahren RSA abgesichert. Es wird lediglich der mit dem Public Key verschlüsselte Geheimtext, und nicht der Klartext gespeichert. Zur Verbindung mit dem jeweiligen System ist die Entschlüsselung des Geheimtextes erforderlich. Dies erfolgt durch den Zugriff auf den Private-Key, welcher sich im Unterverzeichnis \server\standalone\deployments der tenfold-Installation befindet). Der Zugriff auf den Ordner "deployments" ist dementsprechend restriktiv abzusichern (siehe unten)

## 15.4.3 Application Server

### Verzeichnisberechtigungen

Zwei Verzeichnisse innerhalb der tenfold-Installation müssen speziell abgesichert werden. Dieses Absicherung muss nach der Erstinstallation durchgeführt und nach jedem Update überprüft werden. Folgende Verzeichnisse innerhalb der tenfold-Installation sind betroffen (es wird vom Standard-Installationspfad C:\tenfold\ ausgegangen):

- C:\tenfold\server\standalone\deployments (beinhaltet den Private Key zur Entschlüsselung der in der Datenbank verschlüsselt gespeicherten Zugangsdaten für Fremdsysteme)
- C:\tenfold\server\standalone\configuration (beinhaltet gegebenenfalls die Zugangsdaten zur Datenbank, sofern nicht die integrierte Windows Authentifizierung für Microsoft SQL Server gewählt wurde)

Für beide Verzeichnisse gilt, dass die Berechtigungen so eingestellt sein müssen, dass lediglich das tenfold Dienstkonto (das Konto unter dem der Dienst "tenfold Server" läuft) sowie die IT-Administratoren zugreifen dürfen. Es ist lesender und schreibender Zugriff erforderlich.

### Hinweise für Dienstkonten

tenfold führt alle Operationen mit dem jeweiligen Dienstkonto aus. Der Zugriff auf das Dienstkonto muss entsprechend über ein starkes Passwort abgesichert sein. Das Passwort für das Dienstkonto wird in der tenfold Datenbank via RSA verschlüsselt (siehe auch oben). Die Operationen, die über tenfold mit dem Dienstkonto ausgeführt werden, sind seitens der Aufzeichnungen des Fremdsystems (beispielsweise der Ereignisprotokollierung im Active Directory) nicht mehr einem eindeutigen Benutzer zuordenbar. Die Information, wer welche Änderungen beantragt, und letzten Endes freigegeben hat, sind daher dem jeweiligen Request in tenfold zu entnehmen.

## 15.4.4 Netzwerksicherheit

### Verbindung über das Web-Frontend

Verbindungen vom Endanwender mit der tenfold-Oberfläche finden über den Webbrowser statt. Damit der Verkehr zwischen Client und Server nicht abgehört und/oder manipuliert werden kann, muss das HTTPS-Protokoll eingesetzt werden. Die Anleitung zur Konfiguration findet sich unter Technische Sicherheitsinformationen(see page 829). Die Verbindung über HTTP darf nur ausnahmsweise und für

Testzwecke genutzt werden. Für die Authentifizierung des Benutzers gibt es grundsätzlich zwei Möglichkeiten: der Benutzer authentifiziert sich manuell mit seinem Active Directory Benutzernamen und seinem Passwort oder es wird eine automatische Authentifizierung über Kerberos (Single Sign On) durchgeführt (siehe hierzu Technische Sicherheitsinformationen(see page 829)).

### Verbindung zum Active Directory

Die Verbindung von tenfold zum Active Directory erfolgt grundsätzlich über das LDAP-Protokoll. Active Directory erfordert eine verschlüsselte (LDAPS) Verbindung grundsätzlich nur dann, wenn über die Verbindung ein Benutzerpasswort gesetzt werden soll. Es ist in tenfold jedoch möglich und empfohlen, für jede Verbindung LDAPS zu verwenden. Hierzu ist in den Einstellungen der jeweiligen Domäne das Häkchen "SSL erzwingen" zu aktivieren.

### Verbindungen zum tenfold Agent

Die Verbindung zwischen dem tenfold Application Server und dem tenfold Agent erfolgt über Webservices. Die Verbindung ist über HTTPS abgesichert. Es erfolgt eine gegenseitige Verifizierung der Kommunikationspartner, bevor Daten ausgetauscht werden. Das bedeutet, dass der tenfold Server die Identität des Agenten überprüft und umgekehrt, um entsprechende Attacken durch Vorgeben einer falschen Identität auszuschließen.

### Andere Verbindungen

Andere Verbindungen, die tenfold zu Fremdsystemen aufnimmt unterliegen den jeweiligen Richtlinien der Hersteller. Hierfür ist ausschließlich die Dokumentation des jeweiligen Herstellers maßgebend.

## 15.5 Richtlinie zur Behebung von Sicherheits-Bugs

tenfold ist es ein großes Anliegen, sicherzustellen, dass die Systeme von Kunden nicht durch Ausnutzung von Schwachstellen in tenfold kompromittiert werden können.
Aus diesem Grund werden in regelmäßigen Abständen Penetration Tests durchgeführt, um eventuelle Schwachstellen zeitnahe beheben zu können.
Externe Meldungen von Schwachstellen, sei es durch aufmerksame Benutzer, Penetration Tests von Kunden oder externen Sicherheitsfirmen, begrüßen und unterstützten wir in jeglicher Hinsicht.
Wird in tenfold eine Schwachstelle gefunden, ist es in unserem Interesse und im Interesse der Kunden, diese so schnell wie möglich zu beheben.

### 15.5.1 Einstufung und Behebung von Schwachstellen

Zur Kategorisierung von Bugs nutzen wir das Common Vulnerability Scoring System (CVSS Version 2 und Version 3), welches eine transparente Bewertung einer Schwachstelle zulässt.
Wurde eine neue Schwachstelle gemeldet, bemühen wir uns, folgende Zeitrahmen zur Behebung von Sicherheitsproblemen einzuhalten:

- Bugs mit dem Schweregrad **Kritisch** (CVSS v2-Bewertung >= 8, CVSS v3-Bewertung >= 9) sollten spätestens 14 Tage nach der Meldung behoben sein.
- Bugs mit dem Schweregrad **Hoch** (CVSS v2-Bewertung >= 7, CVSS v3-Bewertung >= 7) sollten spätestens 60 Tage nach der Meldung behoben sein.
- Bugs mit dem Schweregrad **Mittel** (CVSS v2-Bewertung >= 3, CVSS v3-Bewertung >= 4) sollten spätestens 180 Tage nach der Meldung behoben sein.
- Bugs mit dem Schweregrad **Niedrig** (CVSS v2-Bewertung < 3, CVSS v3-Bewertung < 4) sollten spätestens 365 Tage nach der Meldung behoben sein.

Diese Zeitrahmen werden jährlich überprüft und bei Bedarf an die sich verändernde Bedrohungslandschaft angepasst.
Wir weisen darauf hin, dass es wichtig ist, immer das neueste tenfold Release in Verwendung zu haben (Best Practice).
Ein Upgrade auf die neueste Version sollte proaktiv durchgeführt werden, um etwaige Schwachstellen schnellstmöglich zu schließen.

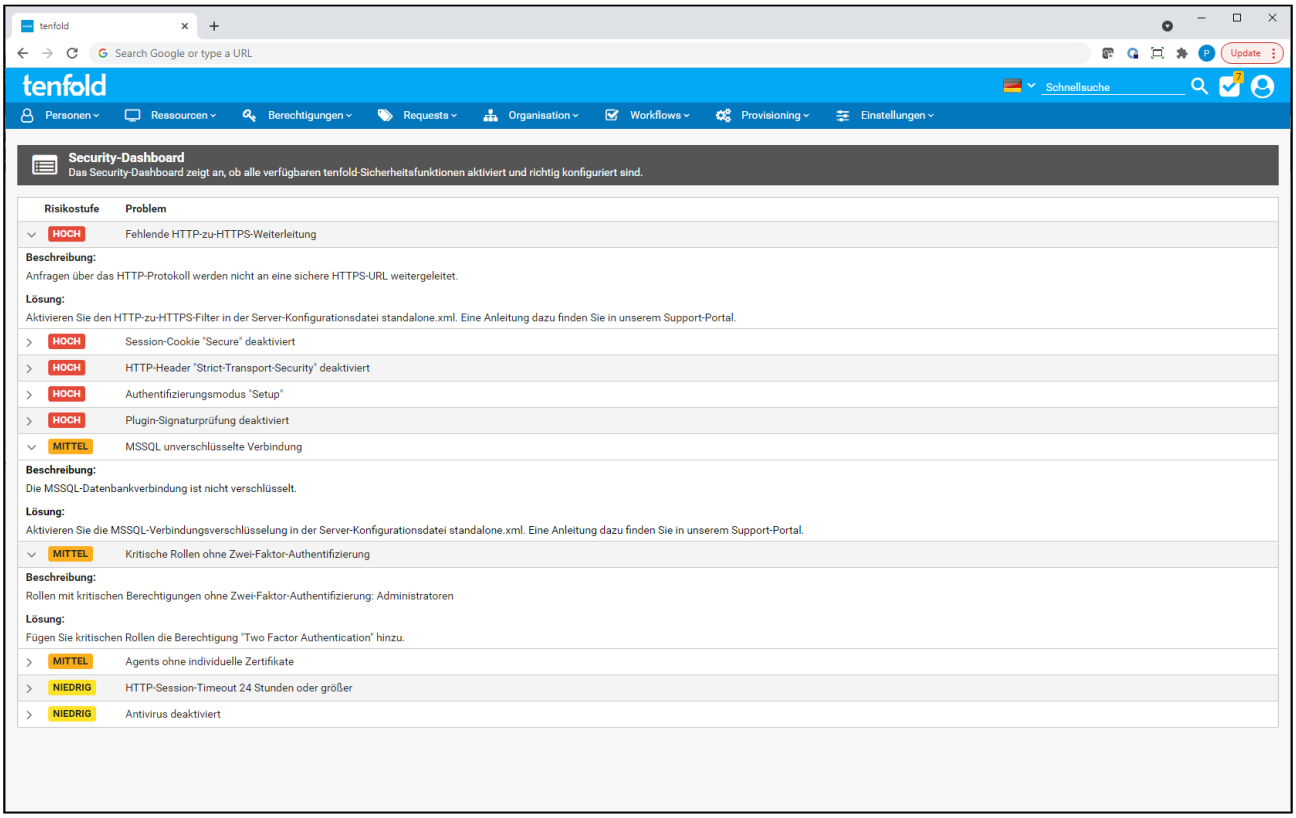
## 15.6 Security Dashboard

tenfold ist eine Andwendung, mit welcher für die Sicherheit Ihrer Umgebung verantwortliche Systeme verwaltet werden. Daher benötigt tenfold an vielen Stellen hohe Berechtigungsstufen. Damit tenfold nicht selbst zu einem Sicherheitsrisiko für Ihre Umgebung wird, gibt es zahlreiche Einstellungen um die Sicherheit von tenfold zu gewährleisten. Mit jeder Version von tenfold kommen hier neue Einstellungen hinzu, um tenfold noch sicherer zu machen und um den immer neueren Bedrohungen Rechenschaft zu leisten.
Um einen Überblick über die stetig wachsende Zahl an Einstellungen zu behalten, bietet tenfold das Security Dashboard, mit welchem Sie einen überblick über sämtliche als unsicher geltenden Einstellungen erhalten.
Näheres zur Bekämpfung von Schwachstellen finden Sie unter Richtlinie zur Behebung von Sicherheits-Bugs(see page 831).

> **Benötigte Berechtigung**
>
> Für den Zugriff auf die Maske wird die Berechtigung "View Security Dashboard" (9110) benötigt.

### 15.6.1 Dashboard Übersicht

Um auf diese Maske zu gelangen, navigieren Sie über das Menü zu Einstellungen > Security > Dashboard.




Auf der Maske angekommen, erhalten Sie einen Überblick über sämtliche Einstellungen von tenfold, welche in ihrem aktuellen Zustand als unsicher eingestuft werden.

> **Updates**
>
> Überprüfen Sie nach jedem Update von tenfold das Dashboard um zu prüfen ob neue Einstellungen hinzugekommen sind. So halten Sie ihr System immer auf dem aktuellsten Stand der Sicherheit.

In dieser Liste finden Sie zunächst eine Auflistung alle Probleme und deren Einstufung.

| Einstufung | Beschreibung | Beispiel |
|---|---|---|
| Hoch | Sämtliche Einträge dieser Einstufung sollten umgehend behoben werden. Ein belassen eines solchen Risikos wird unter keinen Umständen empfohlen, da diese die allgemeine Sicherheit des Systems gefährden. | Der Authentifizierungsmodus ist noch immer als "Setup" eingestellt |
| Mittel | Eine Behebung der Schwachstelle wird prinzipiell empfohlen, kann je nach Systemanforderungen in Absprache mit den Sicherheitsverantwortlichen bestehen bleiben. | Agenten verwenden noch das Standardzertifikat (anstatt eines individuellen Zertifikates) |

| Einstufung | Beschreibung | Beispiel |
| --- | --- | --- |
| Niedrig | Auswirkungen entstehen normalerweise nur in Kombination mit anderen Schwachstellen. Eine Behebung wird dennoch empfohlen. | Die Funktion "Antivirus" ist deaktiviert. |

Zu jedem angeführten Element, können Sie eine detailliertere Beschreibung sowie potentielle Lösungen aufklappen.

> **Sicherheit**
>
> Für eine möglichst hohe Sicherheit, wird empfohlen jeden einzelnen der angeführten Punkte zu beheben.

Im Allgemeinen sollten Sie ein offen lassen von Schwachstellen mit Ihren Sicherheitsbeauftragten besprechen.

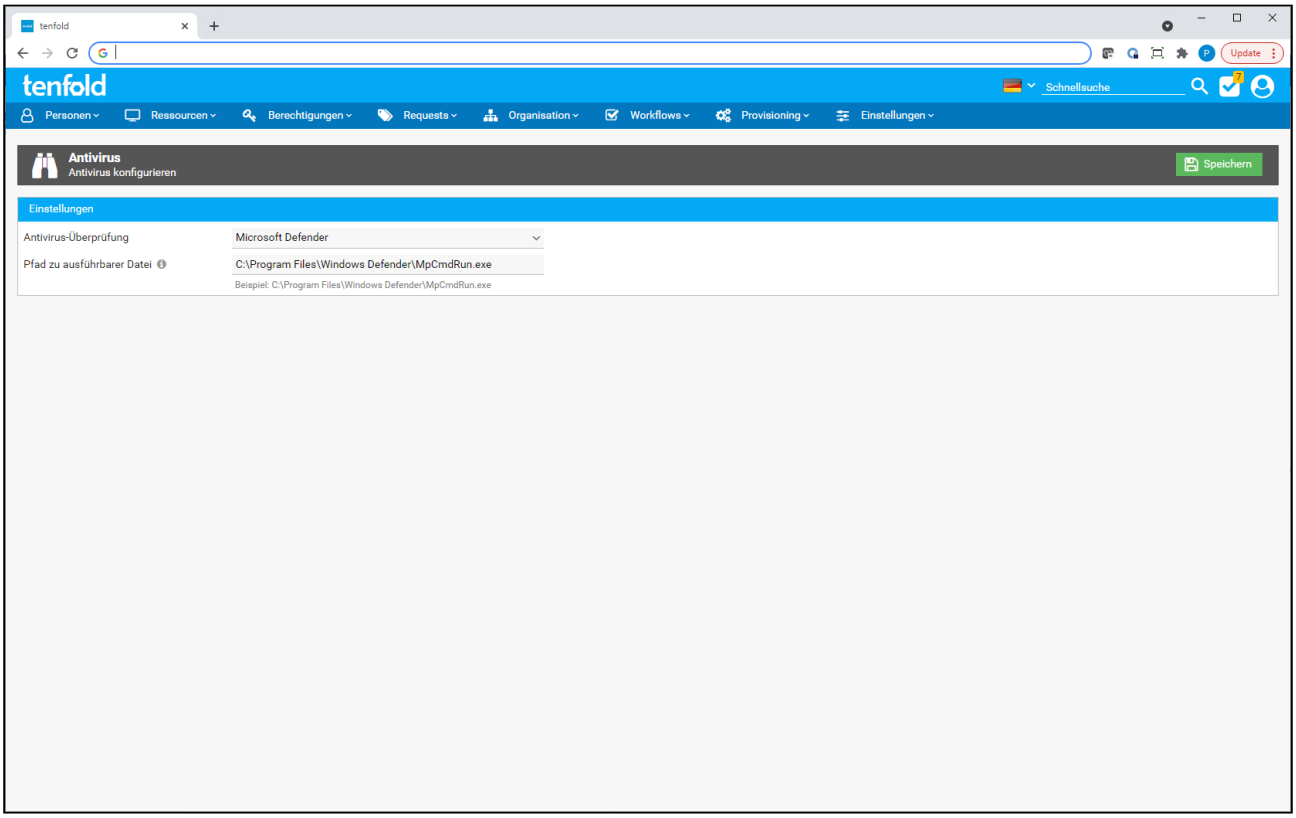
> **Einstufung "Hoch"**
>
> Lassen Sie niemals Schwachstellen der Einstufung "Hoch" offen.

## 15.7 Integration von Antivirus Software

Es ist in tenfold möglich, an verschiedenen Stellen Dateien hochzuladen, um diese anderen Personen zur Verfügung zu stellen.
Um zu gewährleisten, dass hochgeladene Dateien nicht mit Schadsoftware infiziert sind und diese dann an andere Personen verteilt wird, kann Antivirus-Software in tenfold integriert werden, um hochgeladene Dateien zu scannen.

### 15.7.1 Einstellungen

Um die Integration der Antivirus Software durchzuführen, navigieren Sie im Menü auf die Maske *Einstellungen > Security > Antivirus*.




**Benötigte Berechtigung**

Für die Verwaltung ist die tenfold-Berechtigung "Manage Antivirus" (9100) erforderlich.

Auf dieser Maske haben Sie zunächst folgende Einstellungen:

| Einstellung | Beschreibung |
|---|---|
| Antivirus-Überprüfung | Diese Einstellung legt fest, wie tenfold hochgeladene Dateien überprüft. Folgende Auswahlmöglichkeiten stehen zur Verfügung:<br>• **Deaktiviert:** Hochgeladene Dateien werden nicht überprüft.<br>• **Microsoft Defender:** Es wird der von Microsoft integrierte Virenschutz verwendet, um hochgeladene Dateien zu überprüfen.<br>• **Benutzerdefiniert:** Erlaubt es eine beliebige Antivirus Software zu verwenden, welche auf dem tenfold-Server installiert ist. |
| Pfad zu ausführbarer Datei | Geben Sie hier den Pfad zur Ausführbaren Datei des Microsoft Defender an. Diese Einstellung ist nur sichtbar, wenn bei der Einstellung "Antivirus-Überprüfung" die Auswahl "Microsoft Defender" getroffen wurde. |

| Einstellung | Beschreibung |
| --- | --- |
| Kommandozeilenbefehl | Geben Sie hier den Kommandozeilenbefehl an, welcher durchgeführt werden soll, um hochgeladene Dateien auf Schadsoftware zu überprüfen. Richten Sie diesen Befehl entsprechend so ein, dass er entweder im Falle einer positiv getesteten Schadsoftware-Signatur einen Wert ungleich 0 zurückliefert oder die betroffene Datei vom Dateisystem entfernt. Sollte der Befehl 0 liefern und die Datei bestehen bleiben, bedeutet dies für tenfold, dass keine Schadsoftware entdeckt wurde. Benutzen Sie den Platzhalter "${fileName}", um den Pfad der zu prüfenden Datei an die Antivirus-Software zu übergeben. |

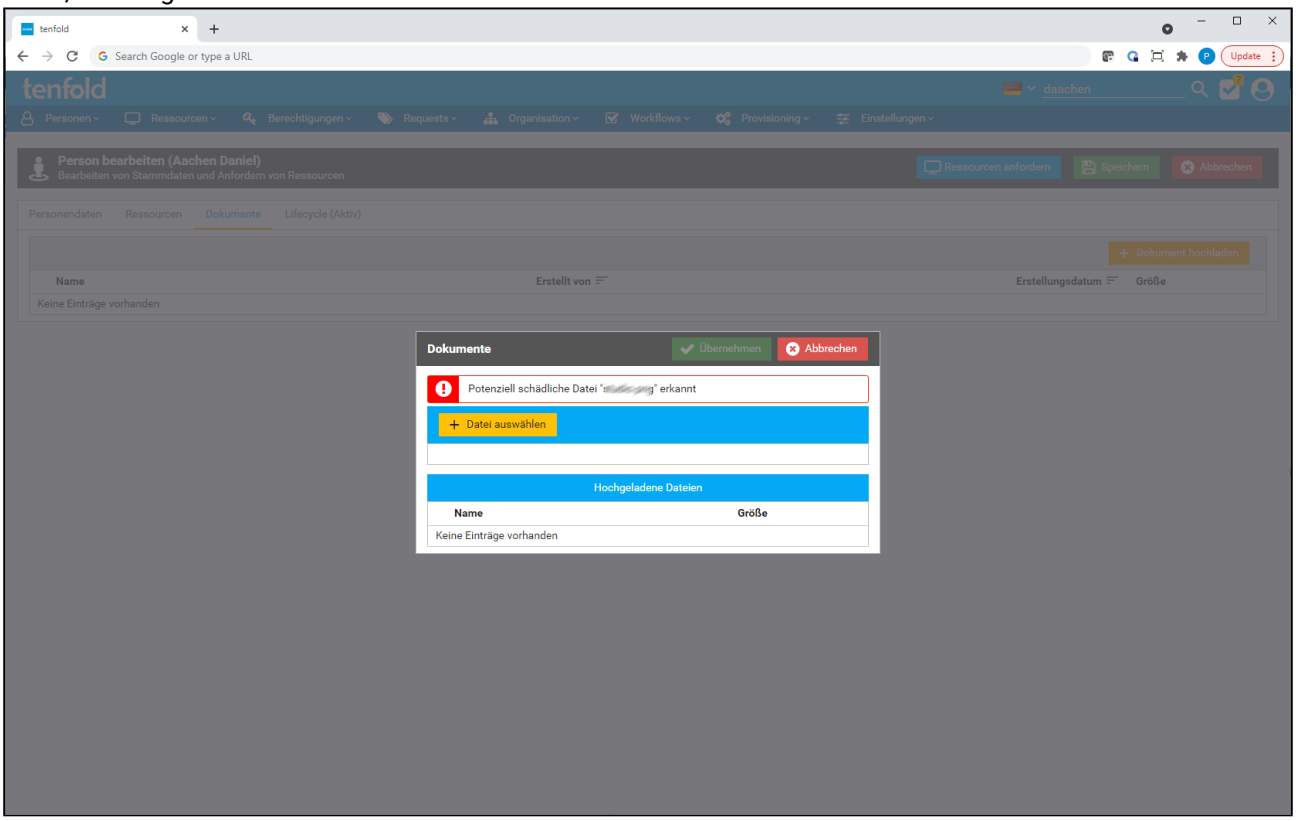
Betätigen Sie die Schaltfläche "Speichern", um die vorgenommenen Einstellungen vorzunehmen.

**Security Dashboard**

Sollte die Auswahl "Deaktiviert" bei der Einstellung "Antivirus-Überprüfung" getroffen worden sein, werden Sie im Security Dashboard (siehe Security Dashboard(see page 832)) auf diesen Umstand hingewiesen.

## 15.7.2 Prüfung von Dateien

Sobald eine Antivirus Software eingerichtet wurde, prüft tenfold jede hochgeladene Datei, egal an welcher Stelle, auf mögliche Schadsoftware.




Sollte in einer Datei Schadsoftware gefunden worden sein, bemängelt tenfold den Upload mit einer Fehlermeldung "Potentiell schädliche Datei <Dateiname> erkannt". In der tenfold Log-Datei wird ebenso ein Eintrag geschrieben, in dem festgehalten wird welcher Benutzer welche möglicherweise schädliche Datei hochgeladen hat.