

Bei den Workflows "Ads request approval", "Ex request approval", "Fs request approval", "O365 group request approval", "O365 license request approval", handelt es sich um Standardgenehmigungsworkflows, welche automatisch auf die jeweiligen Bereiche angewandt werden, solange kein alternative Workflow spezifiziert wurde. Diese Workflows können nicht gelöscht werden.

Wann immer Sie einen Workflow bearbeiten legt tenfold eine neue Revision mit fortlaufender Nummer für diesen Workflow an. Alle aktuell laufenden Genehmigungsprozesse sind von Ihren Änderungen nicht betroffen. Nur Genehmigungsprozesse, welche nach der Änderung starten, folgen dem neuen Schema.

Inaktive Workflows

Sie können im Bereich "Filter" die Einstellung "Auswahlmodus" auf "Alle" ändern und die Schaltfläche "Aktualisieren" betätigen, um die Vorgängerversionen von aktuellen Workflows sowie gelöschte Workflows anzeigen zu lassen. Sie können diese mit der Aktion "Anzeigen" betrachten, jedoch nicht mehr verändern. Sie bleiben revisionssicher abgespeichert.

Gelöschte Workflows in Verwendung

Sie können einen Genehmigungsworkflow jederzeit löschen. Der Workflow wird daraufhin an entsprechenden Stellen nicht mehr zur Auswahl vorgeschlagen, bleibt jedoch an allen Stellen, an denen er verwendet wird, bestehen.

10.3 Kontexte (Workflow)

10.3.1 Hintergrund

Die Kontexte bei Genehmigungsworkflows sind dazu da, um offene Genehmigungen zu gruppieren. Das ist vor allem dann sinnvoll, wenn Benutzer für viele Genehmigungen verantwortlich sind. Kontexte schaffen dann durch die Gruppierung einen besseren Überblick für den Benutzer. Ein Workflow muss dabei nicht zwingend über die gesamte Laufzeit einem Kontext zugeordnet werden. Vielmehr kann der Kontext bei jedem Genehmigungsschritt individuell eingestellt werden.

10.3.2 Verwaltung

Kontexte können über das Menü "Workflows > Kontexte" zentral verwaltet werden.

Benötigte Berechtigung

Für die Verwaltung der Workflow-Kontexte ist die Systemberechtigung "Manage Approval Contexts" (1100) erforderlich.

Genehmigungskontext bearbeiten
Erfassen Sie die gewünschten Stammdaten

Genehmigungskontext

Name * Personenänderung

Beschreibung

Sortiervummer * 10

☐ Ressourcen-Requests gruppieren
☐ Alle genehmigen (Ressource)
☐ Alle genehmigen (Personendaten)
☐ Alle genehmigen (Anwendungsberechtigung)
☐ Alle genehmigen (Lifecycle)
☒ Self-Service Eintrag

Speichern Abbrechen

Folgende Einstellungen müssen bei der Bearbeitung getroffen werden:

Einstellung	Beschreibung
Name	Name für die Darstellung auf der Benutzeroberfläche
Beschreibung	Im Beschreibungsfeld kann der Zweck des Kontext erfasst werden. Dieser Text wird auch auf der Self Service-Oberfläche angezeigt.
Ressourcen-Requests gruppieren	Wenn diese Option aktiviert ist, werden Requests aus diesem Kontext auf der Maske "Requests genehmigen" nach Person gruppiert dargestellt.
Alle genehmigen (unterschiedliche Kategorien)	Diese Option steuert, ob bei der Genehmigung auf der Oberfläche die Schaltfläche "Alle genehmigen" verfügbar ist, mit der alle offenen Requests in diesem Kontext mit einem Klick freigegeben werden können.
Self-Service Eintrag	Mit dieser Einstellung kann man erreichen, dass der Kontext inklusive der Zahl der offenen Requests im Kontext auf der Self Service-Oberfläche als Kachel erscheint. Die Kachel enthält dabei auch die Beschreibung des Kontext sowie den Hinweistext "Genehmigungen"

10.3.3 Einstellungen (Workflow)

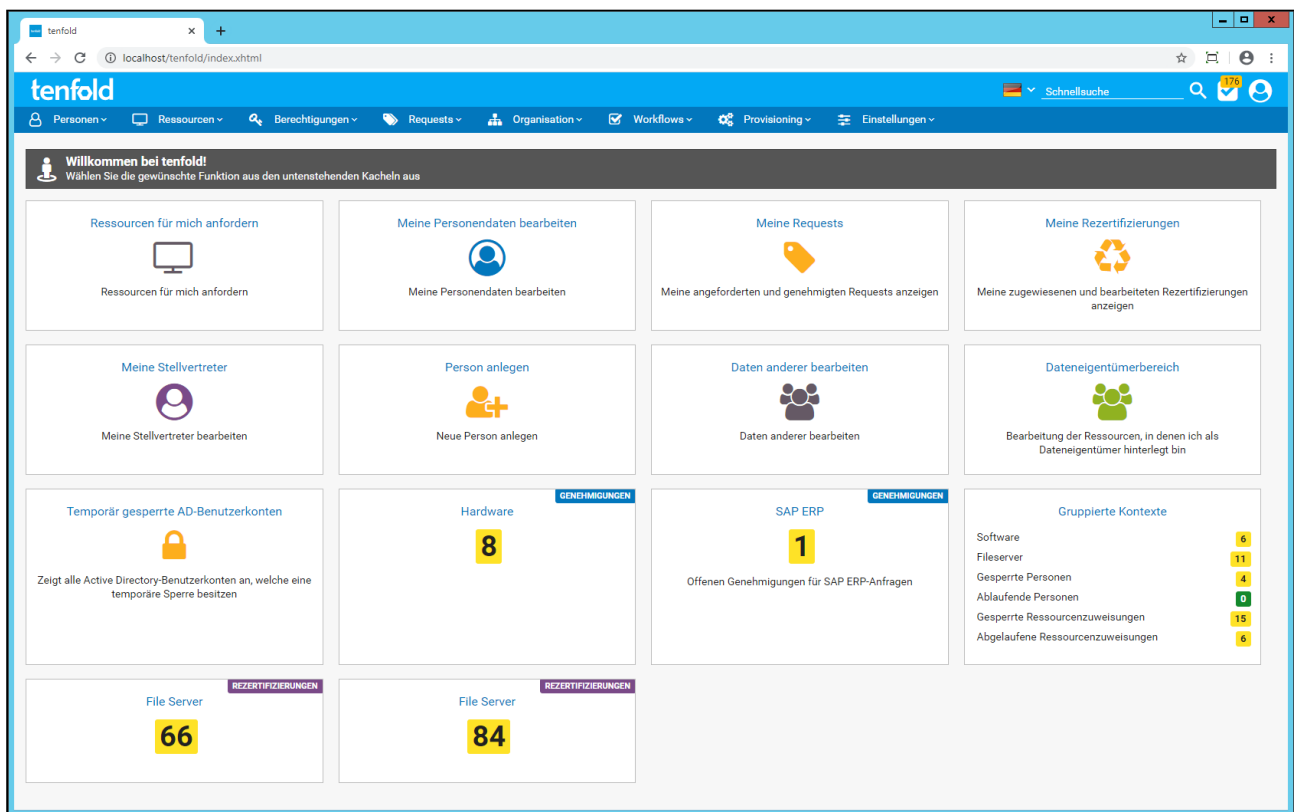
Um den Kontext in einem Genehmigungsworkflow für einen Schritt einzustellen, muss der jeweilige Workflow-Schritt selektiert werden und auf der rechten Seite im Karteireiter "General" unter der Einstellung "Kontext" der gewünschte Kontext ausgewählt werden:

The screenshot displays the tenfold web application interface for editing a workflow. The main header shows the tenfold logo and navigation tabs: Personen, Ressourcen, Berechtigungen, Requests, Organisation, Workflows, Provisioning, and Einstellungen. The current page is titled 'Genehmigungsworkflow bearbeiten (SAP ERP)' with a subtitle 'Erfassen Sie die gewünschten Stammdaten'. Below this, there are three tabs: 'Genehmigungsworkflow', 'Verwendung für Ressourcen-Requests', and 'Verwendung für Personenänderungen'. The 'Allgemein' tab is selected, showing fields for Name (SAP ERP), Revision (1), Vorgänger, Gültig ab (20.06.2018 16:43:06), Gültig bis, and a checkbox for 'Dateianhänge erlauben'. The 'BPMN Modell' section shows a workflow diagram with a task labeled 'SAP ERP Systemeigentümer'. On the right, the 'Task_09v79cy' configuration panel is open, showing the 'General' tab with a dropdown menu for 'Kontext' set to 'SAP ERP'.

10.3.4 Nutzung

Die Kontexte werden an zwei Punkten angezeigt:

- Auf der Self Service-Oberfläche (sofern die Option hierfür aktiviert wurde, siehe oben)
- Durch Klick auf das ToDo-Icon neben der Schnellsuche



10.4 Lifecycle

10.4.1 Grundlagen

Lifecycle-Phasen bilden in tenfold die verschiedenen Zustände ab, in denen sich eine Person befinden kann. Die Standardphase, in der sich eine Person befindet, ist "Aktiv". Zusätzlich sind standardmäßig die Phasen "Gelöscht" und "Gesperrt" definiert. Die Lifecycle-Phasen dienen dazu, automatische Änderungen an Ressourcen- und Berechtigungszuordnungen für Personen durchzuführen, wenn sich diese von einem Zustand in den anderen bewegen.

Lifecycle-Phasen sind nicht dazu geeignet, organisatorische Zuordnungen abzubilden (dafür sollten [Profile](#) (siehe page 168) genutzt werden). Vielmehr sollen mit den Lifecycle-Phasen übergeordnete Änderungen abgebildet werden, wie zum Beispiel längere Abwesenheiten einer Person aufgrund von Elternzeit oder Krankheit, oder beispielsweise das endgültige Ausscheiden aus der Organisation. Die Änderungen, die durch Lifecycle-Phasen an den Zuordnungen einer Person durchgeführt werden, haben gegenüber den Profilen Vorrang. Funktionen, die einen Profilabgleich durchführen, berücksichtigen auch alle Änderungen, die sich durch Veränderungen der Lifecycle-Phasen ergeben haben.

Die Optionen zum Sperren beziehungsweise Löschen einer Person, wie sie aus früheren Versionen von tenfold bekannt sind, wurden durch die Lifecycle-Phasen abgelöst. Neuere tenfold-Versionen sind allerdings abwärtskompatibel, was bedeutet, dass Lifecycle-Phasen in älteren Setups nicht automatisch verfügbar sind. Eine automatische Migration steht aufgrund der Abhängigkeiten zu Legacy-EXECs nicht zur Verfügung. Es ist darüber hinaus dringend empfohlen, die Migration nur von zertifizierten Technikern, gegebenenfalls in Zusammenarbeit mit dem Hersteller, durchführen zu lassen!

10.4.2 Konfiguration

Die Funktion kann im Auslieferungszustand umgehend genutzt werden. Wie oben erwähnt sind drei Phasen bereits vordefiniert. Diese vordefinierten Phasen können nicht gelöscht werden und es wird empfohlen, diese auch nicht anzupassen, außer in Fällen, in denen dies zwingend notwendig ist. Um zur Konfiguration zu gelangen, navigieren Sie im Menü zu *Workflows > Lifecycle*.

Benötigte Berechtigung

Zur Konfiguration der Lifecycle-Phasen ist die Systemberechtigung "Manage Lifecycle Phases" (1124) erforderlich.

Auf den Karteireitern, die nachfolgend beschrieben werden, kann anschließend die Phase bearbeitet werden.

Allgemein

- **Name:** Bezeichnung der Lifecycle-Phase. Sofern keine Übersetzung ausgewählt wurde, wird dieser Name auf der Oberfläche zur Anzeige verwendet.
- **Personen-Request anlegen:** Diese Einstellung ist für spezielle Legacy-Setups erforderlich. Es wird empfohlen, diese Einstellung auf "Keinen Request anlegen" zu setzen, außer in Fällen, wo dies anders erforderlich ist.
- **Icon:** Definiert das Icon für diese Phase, welche unter anderem für die Kachel im Self-Service verwendet wird.
- **Farbe:** Legt die Farbe fest, welche das Icon und die Beschreibung für diese Phase auf der Oberfläche aufweisen.

- **Kommentar erforderlich:** Ist diese Einstellung aktiviert, muss bei allen Requests zu dieser Lifecycle-Phase ein Kommentar eingegeben werden. Diese Einstellung gilt nur für die Maske zur Personenbearbeitung.
- **Passwort-Reset erlaubt:** Legt fest, ob für Personen in dieser Phase die Passwörter zurückgesetzt werden können.
- **Übersetzungs-ID:** Soll die Phasenbezeichnung abhängig von der gewählten Sprache angezeigt werden, so kann hier die entsprechende Übersetzungs-ID hinterlegt werden.
- **Beschriftung:** Wird gesteuert von der Eingabe in der Übersetzungs-ID und zeigt in Worten diese Eingabe in der gewählten Sprache an (z.B. pw_reset.question.10 wird angezeigt als "Was war das Ziel Ihrer ersten Flugreise?")
- **Beschreibung:** Die Beschreibung wird, unter anderem, im Self-Service unterhalb des Icons angezeigt und soll dem Endanwender klar machen, wann diese Phase anzuwenden ist.

In der Tabelle darunter kann festgelegt werden, welche Phasen direkt nach der gerade bearbeiteten Phase zulässig sind. So können bestimmte Übergänge, die ablauftechnisch keinen Sinn ergeben, verhindert werden.

Self-Service

Die Lifecycle-Phasen können auch im Self-Service genutzt werden. Auf diesem Karteireiter können dazu die Einstellungen festgelegt werden:

- **Self-Service für Phase erlauben:** Diese Einstellung steuert, ob die Aktivierung dieser Phase grundsätzlich zur Verfügung steht. Damit ein Benutzer die Phase tatsächlich aktivieren/anfordern kann, müssen dies die Berechtigungen zulassen. Siehe dazu auch weiter unten.
- **Self-Service-Personenbearbeitung:** Mit dieser Checkbox kann man festlegen, ob eine Person, die sich aktuell in dieser Phase befindet, über Self-Service bearbeitet werden darf oder nicht. Typischerweise würde man diese Option in der Phase "Gesperrt" oder ähnlichen Phasen nicht setzen.
- **Kommentar erforderlich:** Ist diese Einstellung aktiviert, muss bei allen Requests zu dieser Lifecycle-Phase ein Kommentar eingegeben werden. Diese Einstellung gilt nur für den Self-Service-Bereich.
- **Ausführliche Beschreibung aktiv:** Steuert, ob der Inhalt im Abschnitt "Ausführliche Beschreibung" angezeigt werden soll oder nicht. Wenn die Option aktiviert ist, kann eine ausführliche Beschreibung (inklusive Formatierung) hinterlegt werden. Diese wird dann im Self-Service vor der Aktivierung der Phase angezeigt (siehe unten). In der ausführlichen Beschreibung sollte ein Text eingegeben werden, der dem Endbenutzer umfangreich erklärt, was beim Aktivieren dieser Phase geschieht.

tenfold

localhost/tenfold/selfservice/self_service_lifecycle_request.html?cid=21&fwid=eMecEq5lgNoEjPXh3Wjpb8OTuMsVqUUYJLI68o:5

tenfold

Personen Ressourcen Berechtigungen Requests Organisation Workflows Provisioning Einstellungen

Lifecycle
Anfordern von Lifecycle

Abbrechen

Neue Lifecycle-Phase anfordern: Elternzeit

Ab in die Elternzeit

Das ist die ausführliche Beschreibung dieser Phase!

Das ist der Text dazu:

- Text
- Text 2
- Text 3

Aktuelle Phase	Aktiv
Angeforderte Phase	Elternzeit
Durchführungszeitpunkt	Sofort
Bemerkung	

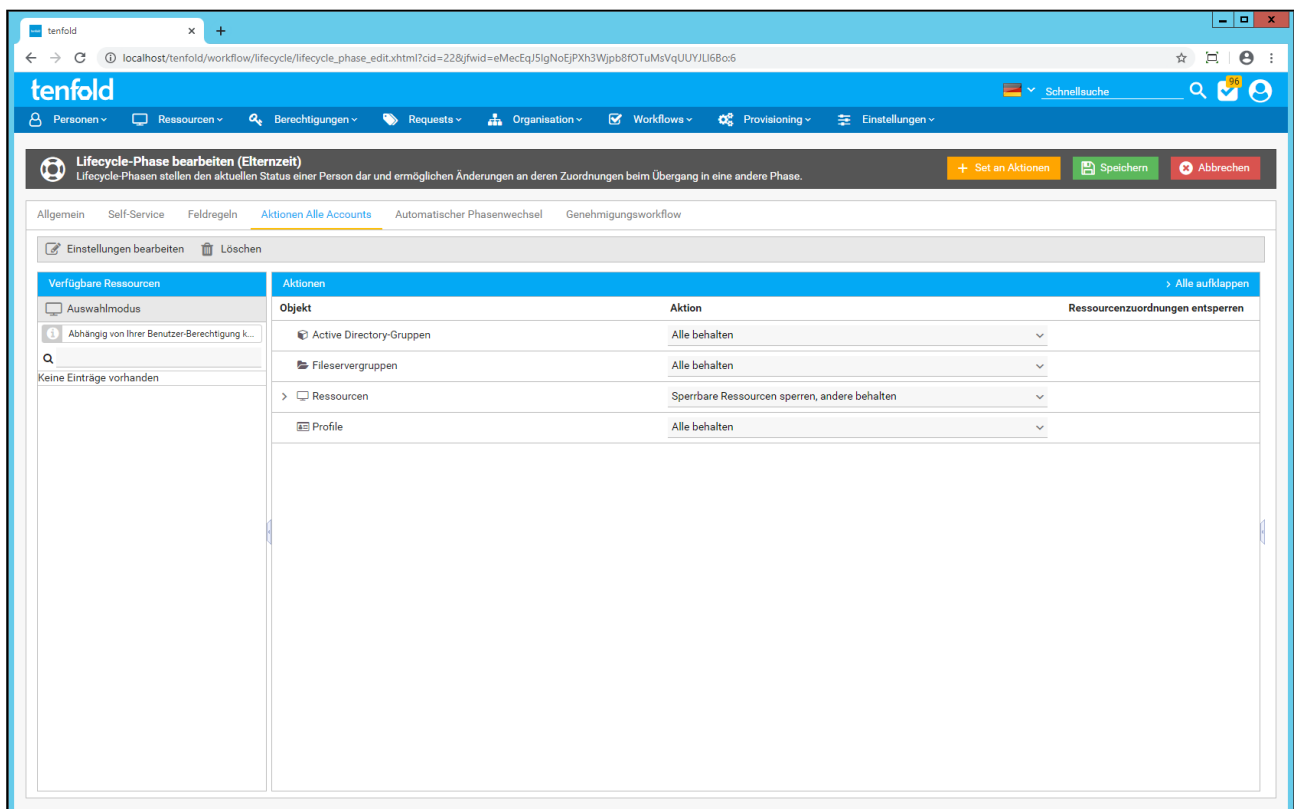
Anfordern

Feldregeln

Im Karteireiter Feldregeln kann gesteuert werden, unter welchen Umständen (siehe [Feldregeln](#)(see page 562)) welches Set an Aktionen ausgeführt werden soll. Zum Beispiel können hier Unterschiede zwischen verschiedenen Personenarten konfiguriert werden, sofern sich die Abläufe beispielsweise zwischen Mitarbeitern und Externen für die gleiche Lifecycle-Phase unterscheiden.

Aktionen

Auf dem Karteireiter Aktionen (welcher pro konfiguriertem Set an Aktionen vorkommt) können die jeweiligen Aktionen für diese Phase konfiguriert werden. Es können pro Phase mehrere unterschiedliche Aktionssets definiert werden. Ein neues Set kann mit dem "+" Button hinzugefügt werden. Welches Aktionsset tatsächlich ausgeführt wird, wird anhand der Feldregeln bestimmt. Die erste Feldregel, die in der Entscheidungstabelle (siehe obiger Punkt "Feldregeln") auf die betreffende Person zutrifft, bestimmt, welches Aktionsset durchgeführt wird. Die Prüfung erfolgt hinsichtlich der Person, für welche die Phase aktiviert werden soll, nicht hinsichtlich der Person, welche die Aktivierung anfordert/durchführt.



Alle Aktionen sind dabei auf unterschiedliche Objekte (siehe untere Tabelle, Spalte "Objekte") aufgeteilt, für welche die Einstellungen individuell festgelegt werden können.

Ausnahmen

Zusätzlich können für jeden Bereich, auf Basis einzelner Ressourcen, Gruppen und Profilen Ausnahmen und Zusatzaktionen angelegt werden. Dazu muss im Auswahlbereich "Verfügbare Ressourcen" das jeweilige Objekt gesucht und anschließend mit Drag & Drop in den Bereich "Aktionen" gezogen werden. So kann man beispielsweise alle zugeordneten E-Mail-Verteilerguppen entfernen, aber gleichzeitig eine bestimmte Verteilergruppe, trotz getroffener Auswahl im Objektbereich, hinzufügen. Die nachfolgende Tabelle unterscheidet dabei zwischen dem Anwendungsbereich "Hauptauswahl" für das Aktionsfeld neben dem Hauptobjekt (zum Beispiel "Active Directory-Gruppen") und "Ausnahme" für individuelle Ressourcen, Gruppen und Profile die auf diesem Wege hinzugefügt oder entfernt wurden.

Folgende grundlegende Möglichkeiten sind dabei vorhanden:

Objekt	Aktion	Beschreibung
Active Directory-Gruppen Hauptauswahl		
	Alle behalten	Bewirkt, dass der Person alle Gruppen, die zum Zeitpunkt der Aktivierung der Phase zugeordnet waren, weiterhin zugeordnet sind.

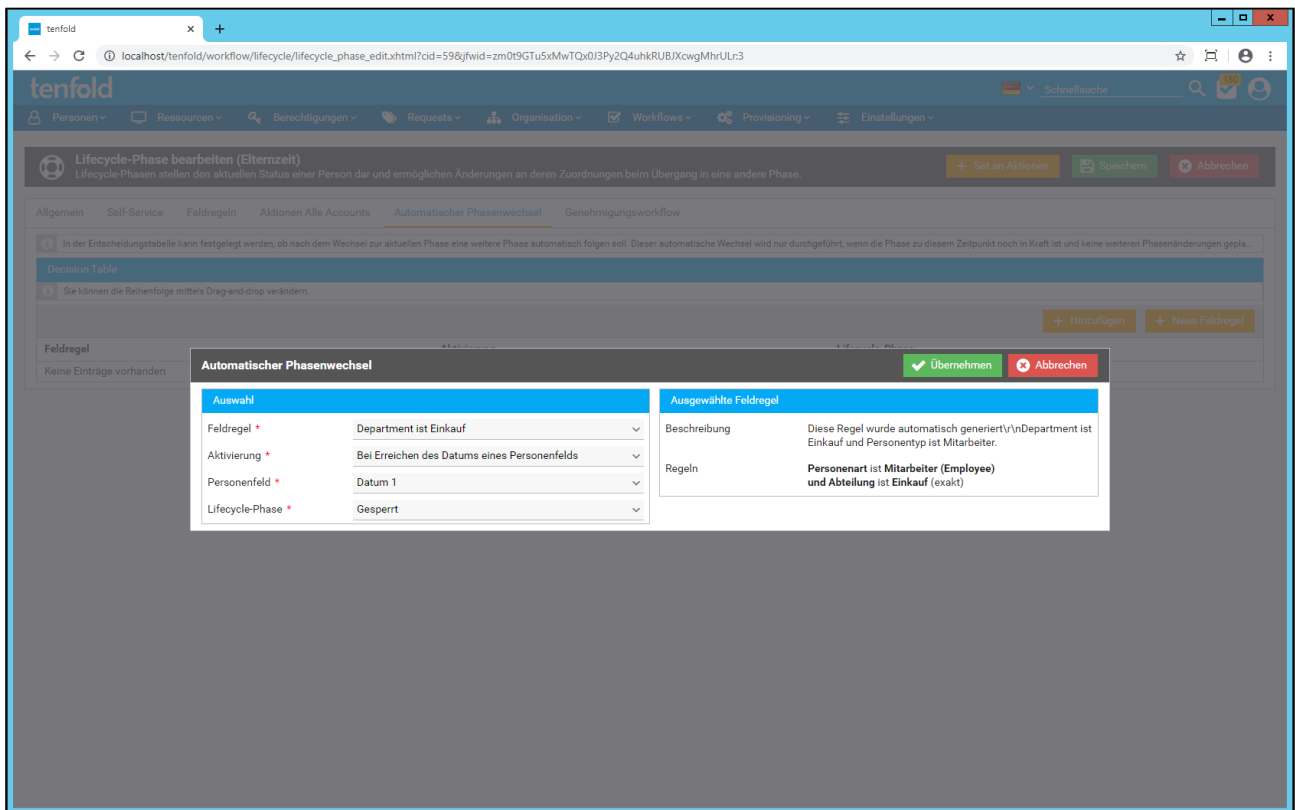
	Alle entfernen	Es werden alle Gruppen entfernt, die zur Aktivierung zugeordnet sind. Die Entfernung betrifft alle der Person zugeordneten Active Directory-Benutzer. Die Primärgruppe der jeweiligen Benutzer wird nicht entfernt.
	E-Mail-Verteilerguppen entfernen	Es werden nur Gruppen vom Typ "Verteilung" entfernt.
Active Directory-Gruppen Ausnahme		
	Entfernen	Die angegebene Active Directory-Gruppe wird entfernt.
	Hinzufügen	Die angegebene Active Directory-Gruppe wird hinzugefügt. Die Gruppe bleibt zugeordnet, auch wenn sich die Phase der Person ändert.
	Hinzufügen (nur für diese Phase)	Die angegebene Active Directory-Gruppe wird hinzugefügt. Wenn sich die Phase der Person ändert, wird die Gruppe wieder entfernt, sofern sie in der nächsten Phase nicht vorgesehen ist.
Fileservergruppen Hauptauswahl		
	Alle entfernen	Alle Fileservergruppen, die der Person zugeordnet sind, werden entfernt. Achtung: Es zählen nur Gruppen als Fileservergruppen, die als solche in tenfold registriert sind.
	Alle behalten	Die Person behält alle zugeordneten Fileservergruppen
Fileservergruppen Ausnahme		
	Entfernen	Die angegebene Fileservergruppe wird entfernt.
	Hinzufügen	Die angegebene Fileservergruppe wird hinzugefügt. Die Gruppe bleibt zugeordnet, selbst wenn sich die Phase der Person ändert.
	Hinzufügen (nur für diese Phase)	Die angegebene Fileservergruppe wird hinzugefügt. Wenn sich die Phase der Person ändert, wird die Gruppe wieder entfernt, sofern sie in der nächsten Phase nicht vorgesehen ist.

Ressourcen Hauptauswahl		
	Alle behalten	Bewirkt, dass der Person alle Ressourcen zugeordnet bleiben.
	Alle entfernen	Bei dieser Einstellung werden alle Ressourcen der Person entfernt.
	Alle entfernen (ohne Request)	Mit dieser Zusatzoption wird bewirkt, dass die Ressourcen entfernt werden, jedoch wird kein Request für die Entfernung angelegt. Damit wird auch das für die Ressource vorgesehene De-Provisioning nicht ausgeführt.
	Sperrbare Ressourcen sperren, andere entfernen	Alle Ressourcen, die der Person zugeordnet und als "Sperrbar" markiert sind (siehe Ressourcenverwaltung (see page 125)) werden gesperrt, alle anderen werden entfernt.
	Sperrbare Ressourcen sperren, andere behalten	Alle sperrbaren Ressourcen, die der Person zugeordnet sind, werden gesperrt, alle anderen bleiben zugeordnet.
Ressourcen Ausnahme		
	Entfernen	Die angegebene Ressource wird entfernt.
	Entfernen (ohne Request)	Die angegebene Ressource wird entfernt. Es wird kein Request für die Entfernung angelegt. Damit wird auch das für die Ressource vorgesehene De-Provisioning nicht ausgeführt.
	Behalten	Der Benutzer behält die angegebene Ressource, sofern sie ihm bereits zugeordnet ist.
	Hinzufügen	Die angegebene Ressource wird hinzugefügt. Die Ressource bleibt zugeordnet, selbst wenn sich die Phase der Person ändert.
	Hinzufügen (nur diese Phase)	Die angegebene Ressource wird hinzugefügt. Wenn sich die Phase der Person ändert, wird die Ressource wieder entfernt, sofern sie in der nächsten Phase nicht vorgesehen ist.
	Sperren	Die angegebene Ressource wird gesperrt, sofern der Benutzer eine Zuordnung für sie hat.
Profile Hauptauswahl		

	Alle behalten	Die Person behält alle ihr zugeordneten Profile.
	Alle behalten, fehlende Inhalte abgleichen	Die Person behält alle ihr zugeordneten Profile. Es findet ein Abgleich statt, sodass Profilelemente, die bei der Person fehlen, automatisch zugeordnet werden.
	Alle entfernen	Es werden alle Profile der Person entfernt. Achtung: Es werden damit auch alle in den Profilen beinhalteten Ressourcen und Gruppen entfernt.
	Manuell zugeordnete entfernen, automatische behalten	Profile, die der Person manuell zugeordnet wurden (ohne automatische Zuweisung, siehe dazu Verwaltung (see page 168)) werden entfernt (mitsamt Ressourcen und Gruppen), aber automatisch zugeordnete bleiben nach wie vor zugeordnet.
Profile Ausnahme		
	Entfernen	Das angegebene Profil wird entfernt.
	Hinzufügen	Das angegebene Profil wird hinzugefügt. Das Profil bleibt zugeordnet, selbst, wenn sich die Phase der Person ändert.
	Hinzufügen (nur für diese Phase)	Das angegebene Profil wird hinzugefügt. Wenn sich die Phase der Person ändert, wird das Profil wieder entfernt, sofern es in der nächsten Phase nicht vorgesehen ist.

Automatischer Phasenwechsel

Der automatische Phasenwechsel bewirkt, dass, unter konfigurierbaren Bedingungen, automatisch eine, von der jeweiligen Phase abweichende, Phase aktiviert wird. Damit lassen sich, zum Beispiel, verzögerte Löschvorgänge abbilden. Es kann z.B., unter bestimmte Voraussetzungen, aus der Phase "Gesperrt" heraus die Phase "Gelöscht" aktiviert werden.



Die Steuerung erfolgt über die Entscheidungstabelle und auf Basis von Feldregeln. Die erste Feldregel, die auf eine Person zutrifft, bestimmt die Einzelheiten zum automatischen Phasenwechsel. Trifft auf keine Person eine der konfigurierten Feldregeln zu, so erfolgt auch kein automatischer Phasenwechsel. Eine Feldregel kann dabei auch mehrmals verwendet werden, um so mehrere verschiedenen Auslöser für den Phasenwechsel zu definieren.

Folgende Einstellungen regeln den Phasenwechsel im Detail:

Einstellung	Beschreibung
Feldregel	Legt fest, welche Attribute die Person aufweisen muss, damit der Wechsel aktiviert wird.

Einstellung	Beschreibung
Aktivierung	<p>Für den Zeitpunkt der Aktivierung gibt es folgende Optionen:</p> <ul style="list-style-type: none"> • Nach x Tag(en) in dieser Lifecycle-Phase • Beim Erreichen des Datums eines Personenfeldes (das Personenfeld muss für die Personenart der betroffenen Person konfiguriert sein und einen Wert aufweisen) • x Tag(e) vor Erreichen des Datums eines Personenfeldes: Das ausgewählte Personenfeld muss für die Personenart der betroffenen Person konfiguriert sein und einen Wert aufweisen. Daraufhin wird der Phasenwechsel eine ausgewählte Anzahl an Tagen vor diesem Datum eingeleitet. • x Tag(e) nach Erreichen des Datums eines Personenfeldes: Das ausgewählte Personenfeld muss für die Personenart der betroffenen Person konfiguriert sein und einen Wert aufweisen. Daraufhin wird der Phasenwechsel zu einer ausgewählten Anzahl an Tagen nach diesem Datum eingeleitet. • Durch Code Snippet: das Snippet muss den richtigen Zeitpunkt ermitteln und anschließend ein Objekt vom Typ <code>java.util.Date</code> zurückliefern, welches das Aktivierungsdatum beinhaltet.
Tage	<p>Setzt die Anzahl an Tagen vor oder nach dem Erreichen eines Datumsfeldes oder der Lifecycle-Phase fest, zu welcher der Phasenwechsel gestartet wird. Diese Einstellung ist nur sichtbar, wenn zuvor "Nach x Tag(en) in dieser Lifecycle-Phase", "x Tag(e) vor Erreichen des Datums eines Personenfeldes" oder "x Tag(e) nach Erreichen des Datums eines Personenfeldes" in der Einstellung "Aktivierung" gewählt wurde.</p>
Personenfeld	<p>Wählen Sie hier das Datumsfeld aus, welches für die Ermittlung des Phasenwechsels herangezogen werden soll. Diese Einstellung ist für die Aktivierungsarten "x Tag(e) vor Erreichen des Datums eines Personenfeldes" und "x Tag(e) nach Erreichen des Datums eines Personenfeldes" sichtbar.</p>
Aktivierung zu bestimmter Uhrzeit	<p>Hiermit kann eingestellt werden, dass der Phasenwechsel zu einer bestimmten Uhrzeit eingeleitet werden soll. Ist die Einstellung inaktiv, so wird der Phasenwechsel um 0:00 durchgeführt.</p>
Uhrzeit	<p>Hier kann zunächst eingestellt werden, ob der Phasenwechsel am Anfang des Tages, am Ende des Tages oder zu einer spezifischen Uhrzeit durchgeführt werden soll. Diese Einstellung ist nur sichtbar, wenn zuvor die Einstellung "Aktivierung zu bestimmter Uhrzeit" aktiviert wurde.</p>
Wert	<p>Legt die spezifische Uhrzeit fest, zu welcher der Phasenwechsel eingeleitet werden soll. Dieses Feld ist nur sichtbar, wenn zuvor die Einstellung "Spezifische Uhrzeit" getroffen wurde.</p>

Einstellung	Beschreibung
Lifecycle-Phase	An diesem Punkt wird die Phase ausgewählt, welche beim Erreichen der Bedingungen aktiviert werden soll.

Genehmigungsworkflow

Im Karteireiter "Genehmigungsworkflow" kann gesteuert werden, welcher Workflow unter welchen Bedingungen für die Erstellung eines Phasenwechsel verwendet wird. Es können dabei folgende Kriterien festgelegt werden:

Einstellung	Beschreibung
Request-Quelle	Zielt darauf ab, aus welcher Quelle der Request erstellt wurde. Bei der Aktivierung über die tenfold-Oberfläche ist die Request-Quelle tenfold. Bei der Aktivierung über das Import Plugin (siehe Import Plugin (see page 710)) gilt die im betreffenden Import definierte Quelle.
Request-Typ	Es kann zwischen der Anforderung eines Phasenwechsels (Neu), der Änderung des Durchführungszeitpunkt (Ändern) oder dem Löschen einer geplanten Aktivierung (Löschen) unterschieden werden.
Genehmigungsworkflow	Legt den anzuwendenden Workflow fest
Automatische Genehmigung-Requests	Wenn diese Option aktiviert ist, werden die aus dem Phasenwechsel resultierenden Requests automatisch genehmigt. Ist die Option nicht aktiviert, so kommen die für die einzelnen Elemente definierten Workflows zum Tragen.

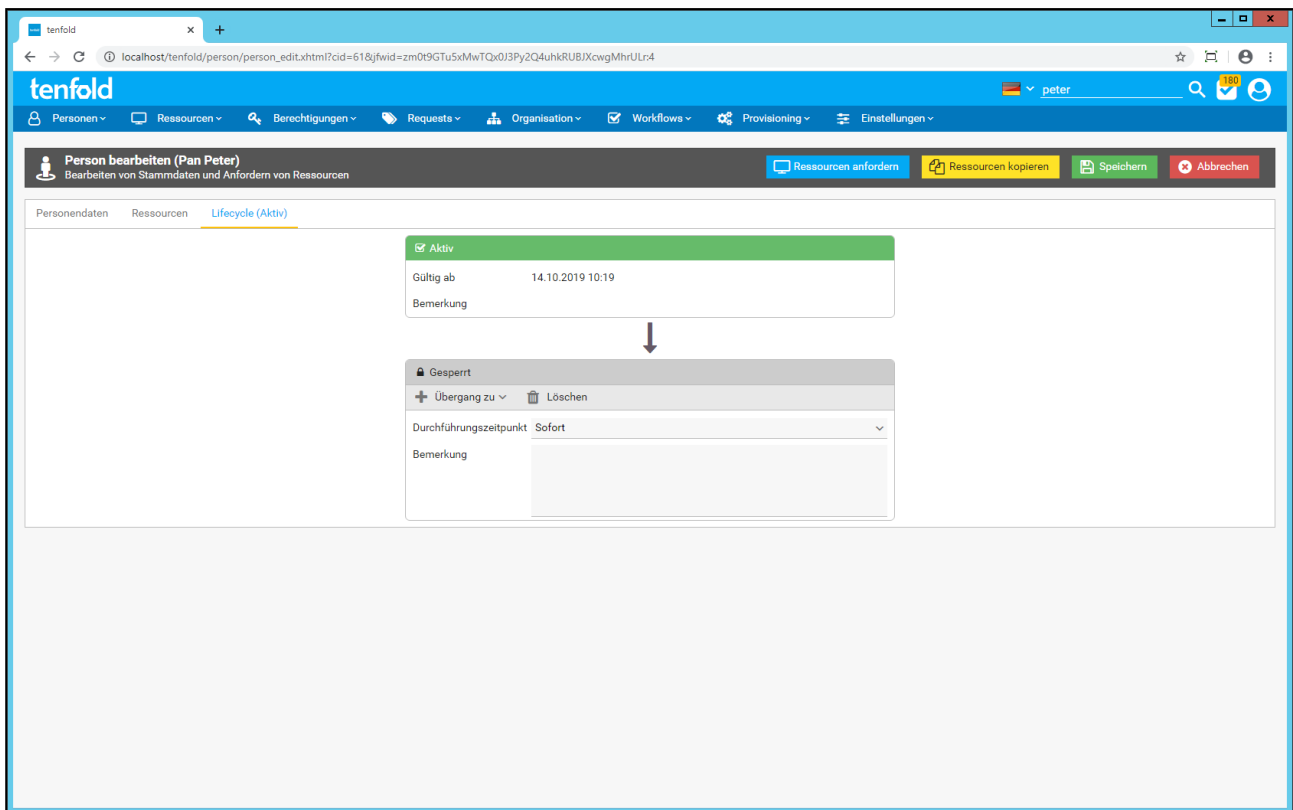
Achtung

In den ausgewählten Genehmigungsworkflows darf der Typ "Dateneigentümer (Ressource)" nicht verwendet werden, da Lifecycle-Phasen keinen Dateneigentümer haben.

10.4.3 Änderungen

Es gibt zwei unterschiedliche Wege, wie die zuvor konfigurierten Phasen bei einer Person aktiviert werden können. Der automatische Phasenwechsel, welcher eine Phase ohne manuelles Zutun auslöst, ist weiter oben beschrieben und wird hier nicht berücksichtigt. Grundsätzlich muss dabei unterschieden werden zwischen dem Einstellen eines Phasenwechsels (welcher in einem Lifecycle-Request vom Typ "Neu" resultiert) und dem tatsächlichen Aktivieren der Phase (dieser Vorgang kann in die Zukunft gelegt werden und erzeugt einen Lifecycle-Request vom Typ "Aktivieren"). Dem Aktivierungs-Request sind alle Requests untergeordnet, welche als Resultat auf den Phasenwechsel erzeugt werden.

Über "Person bearbeiten"



Die erste und umfangreichere Möglichkeit Phasen zu aktivieren bietet die Maske "Person bearbeiten". Auf dem Karteireiter "Lifecycle" können Lifecycle-Phasen für die Person aktiviert werden. Die Überschrift des Karteireiters zeigt zusätzlich immer die aktuelle Phase der Person an.

Ausgehend von der aktiven Phase kann über den Button "Übergang zu" ein Wechsel zu einer anderen Phase eingestellt werden. Es gibt dabei die Möglichkeit, den Wechsel entweder sofort durchzuführen (Durchführungszeitpunkt "Sofort") oder zu einem späteren Zeitpunkt (Durchführungszeitpunkt "Spezifischer Zeitpunkt"). Dazu muss anschließend das gewünschte Datum und die Uhrzeit eingegeben werden. Für die Aktivierung kann eine Bemerkung eingegeben werden.

Auf dieser Maske können gleich mehrere Phasenwechsel geplant werden, in dem in der neu hinzugefügten Phase nochmals der Button "Übergang zu" geklickt und eine der verfügbaren Phasen ausgewählt wird. Die Aktivierung einer Phase kann zeitlich immer nur nach der Aktivierung der vorhergehenden Phase erfolgen.

Benötigte Berechtigung

Für diese Variante sind folgende Berechtigungen erforderlich:

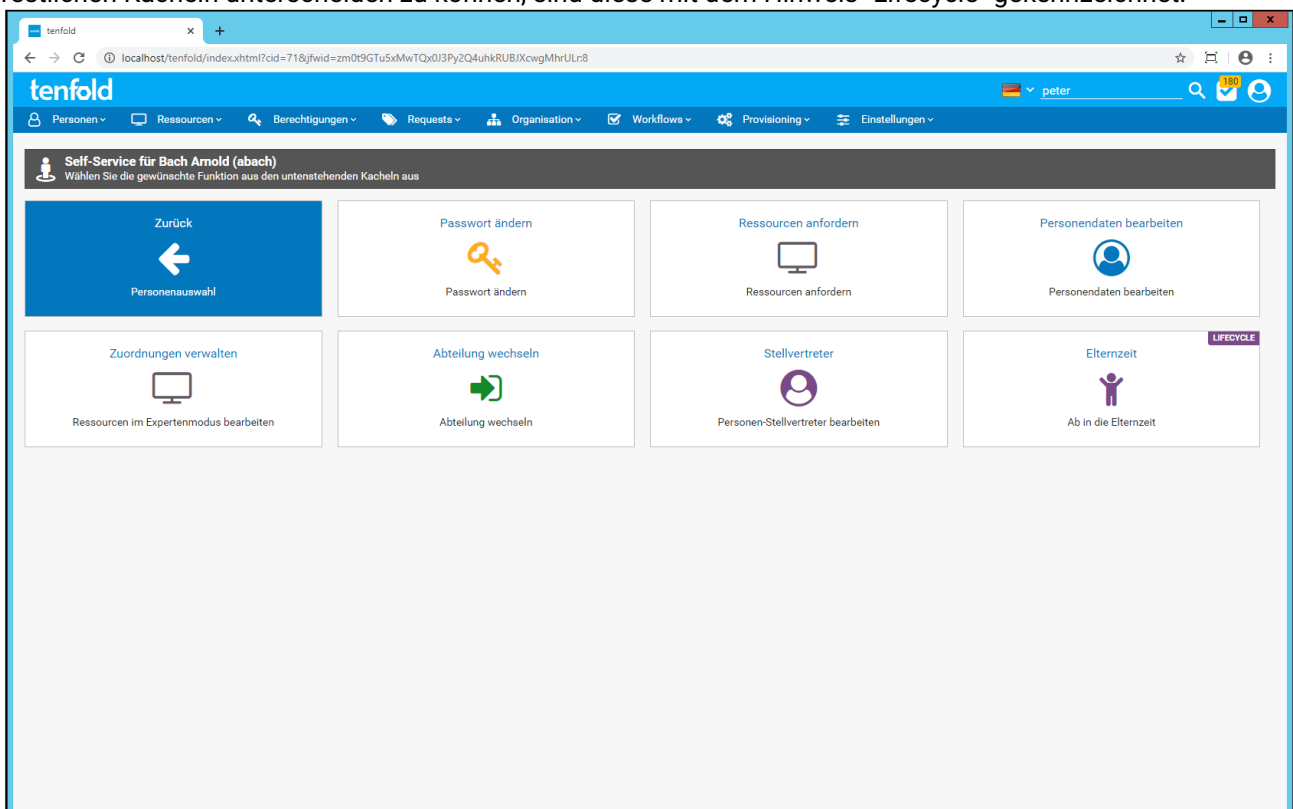
- Für die betreffende Personenart muss in der Rolle die Aktivität "Lifecycle anfordern" freigeschaltet sein. Es muss darauf geachtet werden, dass diese Berechtigung in der Rollenzuordnung auf bestimmte Abteilungen/Niederlassungen/Positionen eingeschränkt werden kann.
- Der Benutzer benötigt darüber hinaus die Systemberechtigung "Edit Person Expert Mode" (2070)

Über Self-Service

Hinweis

Es ist nicht möglich, im Self-Service einen Phasenwechsel für die eigene Person anzufordern!

Die Aktivierung einer Lifecycle-Phase kann auch über die Self-Service-Oberfläche erfolgen. Dazu wählt man auf der tenfold-Startseite die Kachel "Daten anderer bearbeiten" und wählt anschließend die gewünschte Person aus (siehe zum Self-Service auch [Self-Service-Oberfläche](#) (see page 51)). Um die Phasen von den restlichen Kacheln unterscheiden zu können, sind diese mit dem Hinweis "Lifecycle" gekennzeichnet.



Auf der folgenden Maske kann nun mit Klick auf die gewünschte Phase der letzte Schritt der Anforderung gestartet werden.

Hierbei sind folgende Eingaben möglich:

- Der Durchführungszeitpunkt kann analog zur Maske "Person bearbeiten" mit "Sofort" oder einem späteren Zeitpunkt festgelegt werden.
- In der Bemerkung kann eine Begründung für den Phasenwechsel hinterlegt werden.

Mit Klick auf den Button "Anfordern" erfolgt die sofortige Anlage des Phasenwechsel. Sofern kein Genehmigungsworkflow hinterlegt ist, werden die in der Phase konfigurierten Schritte umgehend ausgeführt.

The screenshot shows the tenfold web interface. The top navigation bar includes links for Personen, Ressourcen, Berechtigungen, Requests, Organisation, Workflows, Provisioning, and Einstellungen. The main content area is titled 'Lifecycle' and 'Anfordern von Lifecycle'. It features a form for requesting a new lifecycle phase, specifically 'Elternzeit' (Parental Leave). The form includes a description of the phase, a list of text items, and a table for phase details.

Aktuelle Phase	Aktiv
Angeforderte Phase	Elternzeit
Durchführungszeitpunkt	Sofort
Bemerkung	

At the bottom of the form is a green button labeled 'Anfordern'.

Benötigte Berechtigung

Für die Durchführung eines Phasenwechsels über den Self-Service muss in der Rolle die Aktivität "Lifecycle anfordern" freigeschaltet sein. Es muss darauf geachtet werden, dass diese Berechtigung in der Rollenzuordnung auf bestimmte Abteilungen/Niederlassungen/Positionen eingeschränkt werden kann.

11 Rezertifizierung

Die Rezertifizierung ist ein Prozess, der dazu dient, in regelmäßigen Abständen die Berechtigungen der Benutzer auf ihre aktuelle Notwendigkeit hin zu prüfen. Berechtigungen werden üblicherweise erst zugeordnet, wenn der zuständige Verantwortliche im Rahmen eines Genehmigungsworkflows (siehe [Genehmigungsworkflows](#) (see page 380)) zugestimmt hat. Bei der Rezertifizierung ist der Prozess ein sehr ähnlicher - allerdings mit dem Unterschied, dass der Benutzer die Berechtigung bereits zugeordnet hat und nunmehr entschieden werden muss, ob die Berechtigung auch nach wie vor zugeordnet bleiben soll. In tenfold können alle Arten von Objekten rezertifiziert werden:

- Personen: Kann dazu genutzt werden, um regelmäßig zu kontrollieren, ob eine Person noch aktiv ist oder gesperrt werden kann (zum Beispiel bei externen Dienstleistern)
- Active Directory-Gruppen: Regelmäßige Überprüfung der Zuordnung bestimmter Verteiler- und/oder Sicherheitsgruppen
- Ressourcen: Regelmäßige Kontrolle von Ressourcenzuordnungen, zum Beispiel Anwendungskonten wie SAP
- Anwendungsberechtigungen: Regelmäßige Kontrolle auf Basis einzelner Berechtigungen in Anwendungen (zum Beispiel von Rollen in SAP)

- Profile: Kontrolle der (manuell) zugeordneten Profile.
- Microsoft 365-Gruppen: Überprüfung der Zuordnungen von Gruppen aller Arten, welche in einem Microsoft 365-Mandanten vergeben wurden.
- Microsoft 365-Lizenzen: Regelmäßige Kontrolle, welche Microsoft 365-Lizenzzuordnungen noch notwendig sind.

Die Konfiguration der Rezertifizierung erfolgt über Richtlinien. Wird eine Richtlinie gestartet, so wird das erzeugte Objekt als "Gesamtprozess" bezeichnet. Dieser umfasst alle Personen und Ressourcen die entsprechend der Richtlinie rezertifiziert werden müssen. Jeder Gesamtprozess besteht aus einem oder mehreren Teilprozessen. [Ein Teilprozess steht dabei für alle zu rezertifizierenden Zuordnungen in Verbindung mit einer bestimmten Ressource.](#)

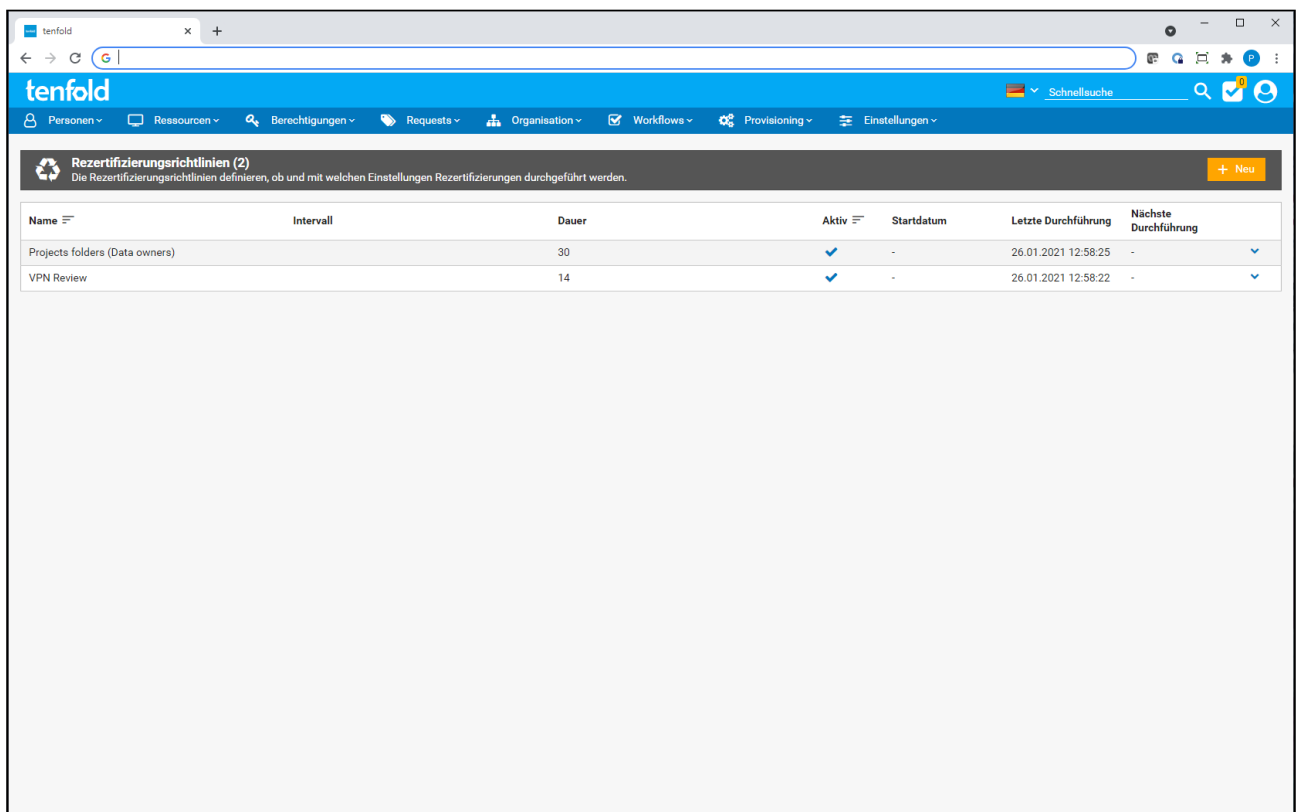
Rezertifizierung und Profile

Seine volle Leistungsfähigkeit entfaltet die Funktion der Rezertifizierung in Verbindung mit Profilen (siehe [Profile\(see page 168\)](#)). Bei der Nutzung von automatisch zugeordneten Profilen werden die Basisberechtigungen, zum Beispiel für eine Abteilung oder eine bestimmte Position, auf Basis von Feldregeln automatisch zugeordnet und wieder entfernt (siehe [Profile\(see page 168\)](#) in Zusammenhang mit [Feldregeln\(see page 562\)](#)). Die in den automatisch zugeordneten Profilen beinhalteten Ressourcen und Berechtigungen müssen somit nicht regelmäßig kontrolliert werden. Die Entfernung von nicht mehr benötigten Berechtigungen erfolgt nämlich automatisch, wenn sich die Feldinhalte derart ändern, dass die zugrunde liegende Feldregel nicht mehr zutrifft. Somit müssen nur Berechtigungen, die nicht über automatisch zugeordnete Profile vergeben wurden, kontrolliert werden.

11.1 Richtlinien

Bevor mit einer Rezertifizierung begonnen werden kann, müssen zunächst Richtlinien zur Rezertifizierung angelegt werden. Mit einer Rezertifizierungsrichtlinie wird festgelegt, welche Personen sowie welche Ressourcen jener Personen, geprüft werden müssen.

Für die Verwaltung der Rezertifizierungsrichtlinien, navigieren Sie über das Menü auf die Maske *Berechtigungen > Rezertifizierung > Richtlinien*.



Name	Intervall	Dauer	Aktiv	Startdatum	Letzte Durchführung	Nächste Durchführung
Projects folders (Data owners)		30	✓	-	26.01.2021 12:58:25	-
VPN Review		14	✓	-	26.01.2021 12:58:22	-

Benötigte Berechtigung

Für die Verwaltung ist die Systemberechtigung "Manage Recertification Policies" (8311) erforderlich.

Es werden Ihnen folgende Informationen zu bestehenden Richtlinien angezeigt:

- Name der Richtlinie
- Intervall
- Dauer
- Status: Aktiv/Inaktiv
- Startdatum
- Zeitpunkt der letzten Durchführung (sofern vorhanden)
- Zeitpunkt der nächsten Durchführung (sofern ein Intervall konfiguriert wurde)

Näheres zu diesen Informationen erfahren Sie im folgenden Abschnitt.

11.1.1 Anlage neuer Richtlinien

Zur Anlage einer neuen Rezertifizierungsrichtlinie, klicken Sie in der Richtlinienliste auf die Schaltfläche "Neu". Sie gelangen daraufhin zur Maske für die Bearbeitung von Rezertifizierungsrichtlinien.

tenfold Rezertifizierungsrichtlinie bearbeiten
Definition der Richtlinie

Allgemein

Name * Beschreibung

Intervall *

Dauer (Tage) *

Aktiv ☒

Bearbeiten ganzer Spalten/Zeilen ☐

Personenkreis

Personenkreis *

Kategorien

[+ Hinzufügen](#)

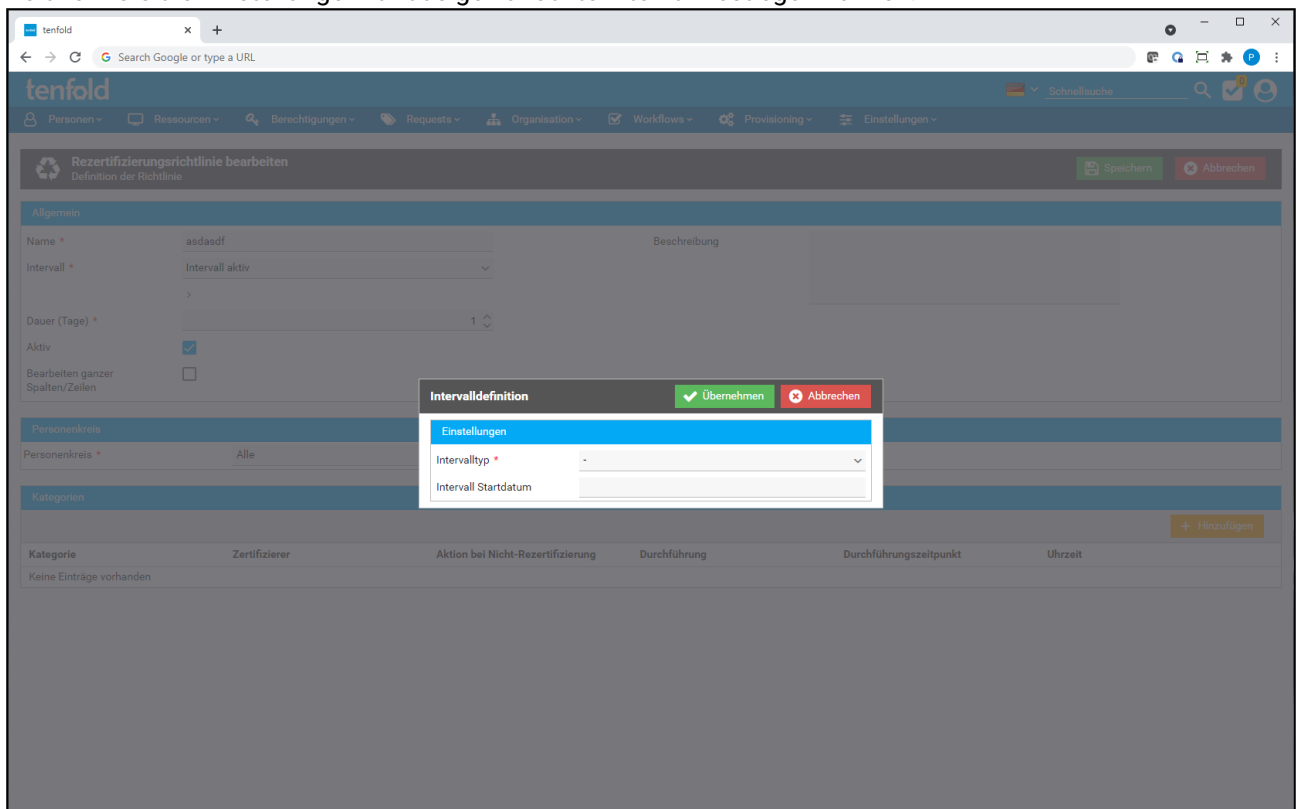
Kategorie	Zertifizierer	Aktion bei Nicht-Rezertifizierung	Durchführung	Durchführungszeitpunkt	Uhrzeit
Keine Einträge vorhanden					

Im Bereich "Allgemein" können Sie zunächst folgende Einstellungen vornehmen:

Einstellung	Beschreibung
Name	Legt den Namen der Richtlinie fest. Diese wird auf den Masken in tenfold angezeigt.
Intervall	<p>Legt fest, in welchem Intervall die Rezertifizierungsrichtlinie gestartet wird. Zunächst sind hier zwei Einstellungen möglich:</p> <ul style="list-style-type: none"> • Nur manuelles Starten: Die Rezertifizierung kann nur manuell, über die Maske zur Verwaltung der Rezertifizierungsrichtlinien, gestartet werden. • Intervall aktiv: Die Rezertifizierung wird in einem regelmäßigen Intervall gestartet. Hinweis: Ein manuelles Starten ist weiterhin möglich. <p>Die genauen Einstellungen für die Intervalle finden Sie im Anschluss.</p>
Dauer (Tage)	Legt die Dauer der Rezertifizierung mit dieser Richtlinie in Tagen fest. Nach Ablauf dieser Zeit wird die Rezertifizierung abgeschlossen und nicht rezertifizierte Berechtigungen werden, je nach Einstellungen, entfernt oder beibehalten.
Aktiv	Diese Einstellung bestimmt, ob eine Richtlinie mit dem nächsten Intervall gestartet wird. Ist diese Einstellung nicht angehakt, so wird keine Rezertifizierung beim Erreichen des nächsten Intervalls gestartet. Hinweis: Ein manuelles Starten ist weiterhin möglich.

Einstellung	Beschreibung
Bearbeiten ganzer Spalten/Zeilen	Erlaubt es, eine Aktion (Rezertifizieren/Nicht rezertifizieren) für ganze Zeilen oder Spalten in der Rezertifizierungsmatrix vorzunehmen, anstatt diese nur auf die einzelnen Objekte anwenden zu können.
Layoutänderung durch Benutzer	Ist diese Einstellung aktiv, kann der Rezertifizierer das Layout während der Bearbeitung ändern. Hinweis: Einzelne Rezertifizierer ändern hierbei das Layout nur für sich selbst während der Bearbeitung.
Beschreibung	Tragen Sie hier eine Beschreibung für die Richtlinie ein, welche Ihnen dabei hilft, Ihre Richtlinien zu organisieren.

Sobald Sie in der Einstellung "Intervall" die Option "Intervall aktiv" gewählt haben, erscheint ein Dialog, in welchem Sie die Einstellungen für das gewünschte Intervall festlegen können.



Zunächst finden Sie zwei Einstellungen vor:

Einstellung	Beschreibung
Intervalltyp	Legt fest, ob das Intervall wöchentlich, monatlich oder jährlich definiert wird.
Intervall Startdatum	Gibt an, ab welchem Datum das Intervall begonnen wird.

Startdatum

Beachten Sie, dass das Startdatum nicht tatsächlich den ersten Tag des Intervalls angibt. Es ist das Datum, ab dem das nächste Intervall gestartet wird.

Beispiel: Sie möchten die Rezertifizierung einmal jährlich am 1. Februar starten. Wenn Sie daraufhin als Startdatum den 1. März des aktuellen Jahres auswählen, so wird die Rezertifizierung das erste Mal am 1. Februar des Folgejahres durchgeführt.

Für wöchentliche Intervalle haben Sie folgende Einstellungsmöglichkeiten:

Einstellung	Beschreibung
Alle x Wochen	Legt fest, wie viele Wochen zwischen den einzelnen Rezertifizierungen liegen.
Wochentag	Legt fest, an welchem Wochentag die Rezertifizierung gestartet wird.

Beispiel:

Alle x Wochen	3
Wochentag	Mittwoch
Intervall Startdatum	01.01.2021
Durchführung	Ab dem ersten Mittwoch des Jahres 2021 und darauffolgend jeden 3. Mittwoch.

Für monatliche Intervalle stehen folgende Optionen zur Verfügung:

Einstellung	Beschreibung
Alle x Monate	Legt fest, wie viele Monate zwischen den Rezertifizierungen liegen.
Tag innerhalb des Monats	Gibt an, an welchem Tag des Monats die Rezertifizierung gestartet wird.

Beispiel:

Alle x Monate	6
Tag innerhalb des Monats	15
Intervall Startdatum	01.01.2021
Durchführung	Erste Durchführung am 15. Jänner 2021 und daraufhin alle 6 Monate am 15. des Monats.

Folgende Einstellungen können für jährliche Durchführung getroffen werden:

Einstellung	Beschreibung
Alle x Jahre	Gibt an, wie viele Jahre zwischen den Rezertifizierungen liegen.
Monat	Legt fest, in welchem Monat die Rezertifizierung durchgeführt wird.

Einstellung	Beschreibung
Tag innerhalb des Monats	Hier wird festgelegt, am wievielten Tag des ausgewählten Monats die Rezertifizierung durchgeführt wird.

Beispiel:

Alle x Jahre	3
Monat	Januar
Tag innerhalb des Monats	12
Intervall Startdatum	01.06.2021
Durchführung	Erste Durchführung am 12. Januar 2022. Daraufhin immer am 12. Februar alle 3 Jahre.

Klicken Sie auf die Schaltfläche "Übernehmen", um die gewünschten Intervalleinstellungen zu akzeptieren.

Mit einem Klick auf die Schaltfläche "Abbrechen" werden die Einstellungen verworfen.

Nachdem Sie die entsprechenden Intervalleinstellungen vorgenommen haben, erscheint, unterhalb der Einstellung "Intervall", ein Link beginnend mit ">" und einer textlichen Beschreibung des Intervalls. Sie können auf diesen Link klicken, um den Dialog für die Intervalleinstellungen erneut zu öffnen, wenn Sie die Einstellungen ändern möchten.

Abbruch

Wenn sie den Dialog bei der ersten Einstellung (versehentlich) abbrechen, erhalten Sie einen Link, welcher nur den Text ">" enthält. Sie können mit diesem Link den Dialog erneut öffnen, um die Einstellungen durchzuführen.

Wenn Sie die allgemeinen Einstellungen durchgeführt haben, fahren Sie fort mit den Einstellungen im Bereich "Personenkreis". Hier kann festgelegt werden, auf welche Personen die Rezertifizierung angewandt wird. Mit diesen Einstellungen lassen sich Szenarien der Rezertifizierung abdecken, in denen nur gewisse Personen berücksichtigt werden müssen. Zum Beispiel kann eine Rezertifizierung nur für Personen bestimmter Personenarten (z.B. externe Mitarbeiter) oder nur für bestimmte Standorte oder Abteilungen durchgeführt werden.

Legen Sie zunächst in der Einstellung "Personenkreis" fest, wie die betroffenen Personen ermittelt werden:

Einstellung	Beschreibung
Alle	Alle Personen sind von dieser Richtlinie betroffen.
Feldregeln	Nur Personen, auf welche ausgewählte Feldregeln zutreffen, sind von der Rezertifizierung betroffen.

Sollten Sie die Option "Feldregeln" gewählt haben, erscheint unterhalb des Menüs eine Tabelle, in welcher Sie Feldregeln bestimmen können, welche zutreffen müssen, damit eine Person in die Rezertifizierung aufgenommen wird.

Warum einschränken?

In der Praxis wird der Personenkreis dann eingeschränkt, wenn z.B. mit dieser Richtlinie nur Mitarbeiter aus bestimmten Abteilungen erfasst werden sollen. Denkbar wäre es auch, mehrere analoge Richtlinien anzulegen, das Intervall aber zu variieren, damit bestimmte kritische Bereiche oder Berechtigungen öfter kontrolliert werden als weniger kritische.

Wählen Sie die Schaltfläche "Neu", um eine bestehende Feldregel hinzuzufügen. Wählen Sie "Neue Feldregel", um direkt auf die Maske zur Erstellung von Feldregeln zu navigieren, um dort eine neue Feldregel anzulegen (siehe [Feldregeln](#) (see page 562)). Sobald Sie die Feldregel gespeichert haben, gelangen Sie automatisch wieder zu der Rezertifizierungsrichtlinie zurück und können die neue Feldregel, wie vorhin beschrieben, hinzufügen.

Mehrere Feldregeln

Sollten Sie mehrere Feldregeln ausgewählt haben, muss eine Person auf **zumindest eine** der ausgewählten Feldregeln zutreffen, um in die Rezertifizierung aufgenommen zu werden. Dies wird durch das Wort "oder" signalisiert, welches in der **zweiten Zeile** jeder **ersten Spalte** steht.

Nachdem definiert wurde welche Personen von der Rezertifizierung betroffen sind, muss noch bestimmt werden, welche Objekte der betroffenen Personen rezertifiziert werden. Dies können Sie im Bereich "Kategorien" festlegen.

Mit der Schaltfläche "Hinzufügen" können beliebig viele Kategorien hinzugefügt werden. Es muss jedoch mindestens eine Kategorie ausgewählt werden, damit eine Rezertifizierung mittels dieser Richtlinie erzeugt werden kann. Nach Betätigung der Schaltfläche öffnet sich ein Dialog, in welchem verschiedene Einstellungen getroffen werden können.

The screenshot displays the 'tenfold' web interface for editing a recertification policy. The main form is titled 'Rezertifizierungsrichtlinie bearbeiten' and includes sections for 'Allgemein' (General), 'Personenkreis' (Person Group), and 'Kategorien' (Categories). A modal dialog titled 'Kategorien' is open, showing a list of categories and options to select a certifier and an action for non-recertification. The background form shows a table for 'Personenkreis' with columns for Name, Company, and Department, and a table for 'Kategorien' with columns for Kategorie, Zertifizierer, Aktion bei Nicht-Rezertifizierung, Durchführung, Durchführungszeitpunkt, and Uhrzeit.

Es finden sich hierbei folgende allgemeinen Einstellungen:

Einstellung	Beschreibung
Kategorie	<p>Legt fest, welche Kategorie von Objekten in der Rezertifizierung berücksichtigt wird. Je nach getroffener Einstellung sind weitere Optionen verfügbar. Folgende Kategorien sind verfügbar:</p> <ul style="list-style-type: none"> • Personen: Rezertifiziert ganze Personen. Verwenden Sie diese Auswahl, wenn es darum geht, komplette Personen, mit allen Berechtigungen und Zugängen, zu rezertifizieren. Zum Beispiel: Für externe Mitarbeiter muss regelmäßig kontrolliert werden, ob diese im anderen Unternehmen noch tätig sind. Wenn nicht, müssen alle Zugänge und Berechtigungen der Person entfernt werden. • Ressourcen: Verwenden Sie diese Einstellung, wenn ganze Anwendungszugänge oder andere Ressourcen (Hardware, etc.) rezertifiziert werden sollen. • Anwendungsberechtigungen: Hiermit können bestimmte Anwendungsberechtigungen rezertifiziert werden, zum Beispiel SAP oder MS Dynamics NAV-Rollen. • Fileserver: Mit dieser Kategorie werden Fileserver-Berechtigungen rezertifiziert. • Active Directory: Hiermit können Sie Active Directory-Gruppenmitgliedschaften rezertifizieren lassen. • Profile: Hiermit können Profilzuordnungen von Personen rezertifiziert werden. • Microsoft 365-Gruppen: Gruppenmitgliedschaften von Microsoft 365-Gruppen werden mit dieser Kategorie rezertifiziert. • Microsoft 365-Lizenzen: Zugeordnete Lizenzen für Microsoft 365-Mandanten werden mit dieser Kategorie rezertifiziert.
Layout	<p>Mit dieser Einstellung kann bestimmt werden, wie das Layout der Rezertifizierungsmatrix aufgebaut ist. Sie haben folgende Einstellungsmöglichkeiten:</p> <ul style="list-style-type: none"> • Rezertifizierungsobjekte in Spalten/Berechtigte in Zeilen • Rezertifizierungsobjekte in Zeilen/Berechtigte in Spalten

Einstellung	Beschreibung
Zertifizierer	<p>Mit dieser Einstellung wird bestimmt, welche Personen in tenfold die Rezertifizierung durchführen. Folgende Einstellungen stehen zur Verfügung:</p> <ul style="list-style-type: none"> • Dateneigentümer: Hiermit müssen die Dateneigentümer der entsprechenden Ressource die Rezertifizierung durchführen. Achtung: Bei dieser Einstellung wird der gewählte Personenkreis ignoriert. Den Dateneigentümern werden immer alle Zuordnungen Ihrer Ressourcen zur Rezertifizierung übergeben. • Abteilungsverantwortliche: Für jede betroffene Person muss der Verantwortliche aus der Abteilung der Person rezertifizieren. • Vorgesetzte: Der jeweilige Vorgesetzte der betroffenen Person muss rezertifizieren. • Berechtigung: Mit dieser Einstellung können Sie eine tenfold-Berechtigung auswählen, welche ein Rezertifizierer besitzen muss, um die Rezertifizierung durchzuführen. Hinweis: Organisationsabhängige Berechtigungen können bei der Zuordnung einer tenfold-Rolle auf bestimmte Teile der Organisation eingeschränkt werden, damit Personen mit der gewählten Berechtigung nicht alle Personen rezertifizieren müssen (siehe Berechtigungen(see page 457)).
Aktion bei Nicht-Rezertifizierung	<p>Stellen Sie hier ein, welche Aktion durchgeführt werden soll, wenn die Rezertifizierung einer Person oder Ressource abgelehnt wird. Im Falle einer erfolgreichen Rezertifizierung bleibt die Zuordnung der Ressource bestehen. Die auswählbaren Aktionen hängen von der ausgewählten Kategorie ab. Es steht jedoch immer die Auswahl "Keine" zur Verfügung. Mit dieser Einstellung passiert, unabhängig davon, ob eine Person/Ressource rezertifiziert wurde oder nicht, gar nichts. Sie können diese Einstellung wählen, um einen Testlauf der Richtlinie durchzuführen, wenn Sie prüfen möchten, ob die Einstellungen Ihren Vorstellungen entsprechen. Damit kann sichergestellt werden, dass durch einen Testlauf keine unerwünschten Nebenwirkungen entstehen. Es könnte, zum Beispiel, ein Abteilungsverantwortlicher nicht wissen, dass es sich nur um einen Testlauf handelt und damit beginnen, Personen die Berechtigungen zu entziehen.</p>
Aktion bei Zeit-Ablauf	<p>Diese Einstellung wird erst sichtbar, wenn Sie eine andere Auswahl als "Keine" in der Einstellung "Aktion bei Nicht-Rezertifizierung" gewählt haben. Hiermit können Sie festlegen, ob, bei Ablauf der Gültigkeitsdauer der Rezertifizierung, die Aktion bei Nicht-Rezertifizierung ausgeführt werden soll oder ob die betroffenen Ressourcenzuordnungen bestehen bleiben sollen.</p>

Einstellung	Beschreibung
Durchführung	<p>Mit dieser Einstellung legen Sie fest, wann die, aus der Rezertifizierung resultierenden Löschvorgänge, durchgeführt werden.</p> <ul style="list-style-type: none"> • Bei Abschluss des Gesamtprozesses • Bei Abschluss eines Teilprozesses <p>Rezertifizierungen bestehen nicht zwangsläufig immer aus einem großen Gesamtprozess. Eine Rezertifizierung für Abteilungsverantwortliche wird, beispielsweise, in Unterprozesse nach den einzelnen Abteilungen aufgeteilt. Mit dieser Einstellung bestimmen Sie, ob die Löschvorgänge für Teilprozesse durchgeführt werden, sobald diese abgeschlossen wurden oder erst dann, wenn alle Teilprozesse abgeschlossen sind.</p> <p>Erst, wenn Sie eine andere "Aktion bei Nicht-Rezertifizierung" als "Keine" gewählt haben, wird diese Einstellung sichtbar.</p>
Durchführungszeitpunkt	<p>Hiermit können Sie einen Zeitpunkt nach Abschluss festlegen, zu welchem die aus der Rezertifizierung resultierenden Löschvorgänge durchgeführt werden. Sie haben die Auswahl zwischen "Sofort nach Abschluss" oder "Zu bestimmter Uhrzeit".</p> <p>Mit der Einstellung "Sofort nach Abschluss", werden die Löschvorgänge durchgeführt, sobald der Teilprozess oder Gesamtprozess (je nach Auswahl in der Einstellung "Durchführung") abgeschlossen sind. Mit "zu bestimmter Uhrzeit" wird gewartet, bis das nächste Mal die eingetragene Uhrzeit erreicht wird. Achtung: Da die Durchführung der Löschvorgänge potentiell länger andauern kann bzw. viele Ressourcen in den betroffenen Systemen in Anspruch nehmen kann, wird empfohlen, eine Uhrzeit zu wählen, in der die Systeme wenig belastet sind.</p> <p>Diese Einstellung ist erst sichtbar, wenn Sie eine andere "Aktion bei Nicht-Rezertifizierung" als "Keine" gewählt haben.</p>
Genehmigungsmodus	<p>Nach der Rezertifizierung werden für alle durchzuführenden Aktionen entsprechende Requests angelegt, wie sie auch in den meisten anderen Fällen von tenfold angelegt werden. Mit dieser Einstellung können Sie auswählen, ob diese Requests automatisch genehmigt werden sollen oder ob die üblichen Genehmigungsworkflows erforderlich sind.</p>

Nicht gesetzte Daten

Wird in den Einstellungen ein Zertifizierer gewählt, der in einem konkreten Fall nicht existiert (zum Beispiel wird "Dateneigentümer" gewählt und eine bestimmte Active Directory-Gruppe hat keinen Dateneigentümer), so werden die auf diesen Fall zutreffenden Ressourcen bei der Rezertifizierung einfach nicht berücksichtigt (die Active Directory-Gruppe ohne Dateneigentümer würde somit nicht in dem jeweiligen Prozess zur Rezertifizierung vorhanden sein).

Automatische Profilzuordnungen

Automatische Profilzuordnungen und Zuordnungen von Objekten, welche durch automatische Profilzuordnungen entstanden sind, sind von Rezertifizierungen ausgeschlossen.

Je nach ausgewählter Kategorie haben Sie noch weitere Einstellungsmöglichkeiten, um die Rezertifizierung weiter einzuschränken, bzw. sind weitere Aktionen verfügbar.

Kategorie	Einstellung	Beschreibung
Personen	Aktion bei Nicht-Rezertifizierung	Folgende Aktionen stehen zur Auswahl: <ul style="list-style-type: none"> • Personen-Request: Erstellt einen Request zur Löschung oder Sperrung der Person. • Lifecycle-Phase ändern: Lässt die Person in eine andere Lifecycle-Phase wechseln. Sollten Sie Lifecycle-Phasen verwenden, wird empfohlen, diese Option auszuwählen.
	Personen-Request	Diese Einstellung legt fest, welche Art von Personen-Request erzeugt werden soll, wenn in der obigen Einstellung die Auswahl "Personen-Request" getroffen wurde. Sie können einen Sperren-Request oder Löschen-Request anlegen lassen.
	Lifecycle-Phase	Bestimmt die Lifecycle-Phase, in welche die Person verschoben werden soll, sollten Sie als Aktion "Lifecycle-Phase ändern" ausgewählt haben.
Ressourcen	Einschränkung	Hiermit können Sie festlegen, ob alle Ressourcen der gewählten Kategorie rezertifiziert werden sollen oder ob Sie die Auswahl auf bestimmte Ressourcen einschränken möchten.
	Aktion bei Nicht-Rezertifizierung	Mit dieser Einstellung können Sie auswählen, ob die Ressourcenzuordnung der betroffenen Person bei Nicht-Rezertifizierung gesperrt oder gelöscht werden soll.
Andere Kategorien	Einschränkung	Analog zur Kategorie "Ressourcen" kann hier eingestellt werden, ob die Rezertifizierung auf alle Objekte der gewählten Kategorie angewandt werden soll oder nur auf bestimmte.
	Aktion bei Nicht-Rezertifizierung	Für die anderen Kategorien steht, neben "Keine", nur die Aktion "Löschen" zur Verfügung. Hierbei wird das Objekt der Person entzogen.

Sollten Sie in der Einstellung "Einschränkung" verschiedener Kategorien die Auswahl "Auf bestimmte Objekte einschränken" getroffen haben, so erscheint unterhalb des Bereichs "Kategorien" ein weiterer Bereich, "Einschränkung". Wählen Sie in diesem Bereich in der Auswahl das gewünschte Objekt aus und klicken Sie auf die Schaltfläche "Hinzufügen", um das Objekt zur Rezertifizierung hinzuzufügen.

Im Falle von Fileserver-Berechtigungen haben Sie, bei den Einstellungen für die Einschränkung auf bestimmte Verzeichnisse, noch eine weitere Option: "Unterverzeichnisse". Mit dieser kann bestimmt werden, wie mit den Unterverzeichnissen der ausgewählten Verzeichnisse umgegangen werden soll. Sie haben folgende Auswahlmöglichkeiten:

- **Unterverzeichnisse ausschließen:**

Es werden nur die ausgewählten Verzeichnisse rezertifiziert. Etwaige Unterverzeichnisse von diesen werden ignoriert.

- **Unterverzeichnisse ohne Dateneigentümer einschließen:**

Es werden die ausgewählten Verzeichnisse rezertifiziert, so wie all jene Unterverzeichnisse, auf welchen keine Dateneigentümer gesetzt sind. Dies entspricht den normalen Regeln des Zuständigkeitsbereiches eines Dateneigentümers, welcher ebenso nur Unterverzeichnisse ohne gesetzten Dateneigentümern einschließt.

- **Alle Unterverzeichnisse einschließen:**

Alle ausgewählten Verzeichnisse und deren Unterverzeichnisse sind Teil der Rezertifizierung.

In der darunter befindlichen Tabelle können Sie, im Aktionsmenü der jeweiligen Zeile, mit der Aktion "Löschen" das gewählte Objekt wieder aus der Rezertifizierung entfernen.

Nachdem Sie alle Einstellungen getroffen haben, schließen Sie die Konfiguration der Richtlinie mit einem Klick auf die Schaltfläche "Speichern" ab.

11.1.2 Weitere Aktionen

Unter *Berechtigungen > Rezertifizierung > Richtlinien* stehen Ihnen weitere Aktionen für die Richtlinien im Aktionsmenü des jeweiligen Eintrages zur Verfügung.

Name	Intervall	Dauer	Aktiv	Startdatum	Letzte Durchführung	Nächste Durchführung
Projects folders (Data owners)		30	✓	-	26.01.2021 12:58:25	
VPN Review		14	✓	-	26.01.2021 12:58:22	

Aktion	Beschreibung
Bearbeiten	Mit dieser Aktion werden bestehende Richtlinie bearbeitet. Achtung: Änderungen einer Richtlinie haben keine Auswirkungen auf laufende Rezertifizierungsprozesse, die nach dieser Richtlinie erstellt wurden.

Aktion	Beschreibung
Löschen	Löscht eine bestehende Richtlinie. Achtung: Das Löschen einer Richtlinie hat keine Auswirkungen auf laufende Rezertifizierungsprozesse, die nach dieser Richtlinie erstellt wurden. Einmal gelöschte Richtlinien können nicht wiederhergestellt werden.
Deaktivieren	Deaktiviert eine Richtlinie vorübergehend. Dies bewirkt, dass kein Prozess beim Eintreten des nächsten Intervalls erzeugt wird. Diese Aktion hat denselben Effekt, wie wenn die Richtlinie bearbeitet wird und dort der Haken bei der Einstellung "Aktiv" entfernt wird.
Aktivieren	Reaktiviert eine nicht aktive Richtlinie. Diese Aktion hat denselben Effekt, wie wenn eine Richtlinie bearbeitet wird und dort der Haken bei der Einstellung "Aktiv" gesetzt wird.
Starten	Startet sofort einen Rezertifizierungsprozess, basierend auf dieser Richtlinie. Dies kann unabhängig von Intervalleinstellungen geschehen und die Richtlinie muss hierfür auch nicht aktiv sein.

11.2 Rezertifizierungsprozesse

Nachdem eine Richtlinie (siehe Richtlinien) erstellt wurde, können, anhand dieser, Prozesse zur Rezertifizierung von Objekten gestartet werden. Bei diesen Objekten kann es sich um ganze Personen handeln oder um einzelne Zuordnungen von Ressourcen, Active Directory-Gruppen, Berechtigungen, etc. Welche Personen und Zuordnungen von der Rezertifizierung betroffen sind, hängt von den Einstellungen in der jeweiligen Richtlinie ab.

Sobald ein Prozess gestartet wurde, haben die eingetragenen Rezertifizierer eine gewisse Anzahl an Tagen, um die Inhalte des Prozesses zu rezertifizieren.

Hierbei erhalten die Rezertifizierer eine Liste an Objekten und müssen entweder bestätigen, dass die Objektzuordnung rezertifiziert wird (Objekt bleibt erhalten) oder, dass diese nicht rezertifiziert wird (Aktion ist abhängig von den Einstellungen der Richtlinie).

11.2.1 Übersicht der Prozesse

Für eine Übersicht von allen jemals gestarteten Prozesse, navigieren Sie über das Menü auf die Maske *Berechtigungen > Rezertifizierung > Übersicht*.

tenfold

Personen Ressourcen Berechtigungen Requests Organisation Workflows Provisioning Einstellungen

Überblick
Zeigt aktuelle und historische Rezertifizierungen

Filter

Von 09.07.2021 Status *
Bis 08.08.2021 Rezertifizierungsrichtlinie -

Aktualisieren

Rezertifizierungsrichtlinie	Beschreibung	Startdatum	Enddatum	Status	Fortschritt
VPN Review		09.07.2021	23.07.2021	OFFEN	0 / 1 (0,0%)
Ressource: VPN	Ressourcen			OFFEN	0 / 2 (0,0%)

Benötigte Berechtigung

Für die Übersicht wird die Systemberechtigung "View Recertifications" (8310) benötigt.

Wenn Sie die Maske betreten, werden Ihnen alle gestarteten Rezertifizierungsprozesse angezeigt, welche im Zeitraum des aktuellen Tages bis einen Monat später gültig sind. Sie können im Bereich "Filter" den Gültigkeitszeitraum verändern und mit der Schaltfläche "Aktualisieren" die anzuzeigenden Prozesse neu laden. Ebenso können Sie mit dem Filter "Status" auf nur laufende oder nur abgeschlossene Prozesse filtern und mit der Einstellung "Rezertifizierungsrichtlinie" jene Prozesse filtern, die auf einer bestimmten Richtlinie basieren.

Die Einstellungen der Datumsfelder "Von" und "Bis" legen fest, in welchem Zeitraum die Rezertifizierung gelaufen ist. Es werden also jene Rezertifizierungen berücksichtigt, wo entweder das Startdatum oder das Enddatum in diesem Bereich liegen.

In der Tabelle finden Sie die Rezertifizierungsprozesse. Sie können diese Prozesse aufklappen, um sich die Teilprozesse anzeigen zu lassen. Prozesse werden, je nach Kategorie, in Teilprozesse aufgegliedert. Beispielsweise wird bei Ressourcen für jede zu rezertifizierende Ressource ein Teilprozess gestartet. Im Aktionsmenü von jedem Prozess oder Teilprozess haben Sie die Möglichkeit, sich diesen entweder anzeigen zu lassen oder ihn abubrechen.

Benötigte Berechtigung

Für das Abbrechen von Rezertifizierungsprozesse wird die Systemberechtigung "Cancel recertifications" (8312) benötigt.

Über diese Maske lassen sich, unabhängig von der Zuständigkeit der Rezertifizierung, alle Prozesse und deren Ergebnisse betrachten. Sie können in die Prozesse jedoch nur dann eingreifen, wenn Sie durch die Richtlinie als Rezertifizierer eingetragen sind (siehe Richtlinien).

Sie sehen an dieser Stelle eine Matrix mit allen zu rezertifizierenden Objekten. Wie diese Matrix aufgebaut ist, hängt vom eingestellten Layout der Richtlinie ab.

Layout	Beschreibung
Rezertifizierungsobjekte in Spalten/ Berechtigte in Zeilen	In jeder Zeile wird der Inhaber einer Zuordnung angezeigt. In den Spalten werden die jeweiligen Objekte (tenfold-Ressourcen, Active Directory-Gruppen, etc.) angezeigt.
Rezertifizierungsobjekte in Zeilen/ Berechtigte in Spalten	In dieser Layout-Variante gibt es für jede Ressource (tenfold-Ressourcen, Anwendungsberechtigungen, etc.), die im Bereich der Rezertifizierung liegt, eine Zeile. In den Spalten befinden sich die jeweiligen Besitzer der Ressourcenzuordnungen.

Layout ändern

Ist in der Rezertifizierungsrichtlinie die Einstellung "Layoutänderung durch Benutzer" aktiv, kann der Benutzer das vorgegebene Layout durch die Schaltfläche "Zeilen/Spalten tauschen" ändern. Dies wirkt sich nur auf die aktuelle Ansicht des angemeldeten Benutzers aus.

Sollte der Prozess bereits zur Gänze oder in Teilen rezertifiziert worden sein, so erkennen Sie dies ebenso an den farblich hervorgehobenen Schaltflächen.

The screenshot shows the 'tenfold' web application interface. The main header includes navigation links: Personen, Ressourcen, Berechtigungen, Requests, Organisation, Workflows, Provisioning, and Einstellungen. The current page is titled 'Rezertifizierung anzeigen - VPN Review' with a subtitle 'Anzeige des aktuellen bzw. historischen Status eines Gesamt- oder Teilprozesses einer Rezertifizierung.' and a 'Zurück' button.

On the left, there is a sidebar with 'Kategorien' (Ressourcen 2) and 'Rezertifizierung' (Name: VPN Review, Beschreibung: Startdatum: 07/09/2021, Enddatum: 07/23/2021).

The main content area features a 'Filter' section with dropdowns for Status, Abteilung, and Ressource, and a checkbox for 'Nur Zeilen mit sichtbaren Rezertifizierungen anzeigen' (checked). Below the filters is a table with columns for 'Object' and 'VPN'.

Object	VPN
Maradona Diego (dmaradon) Accounting	<input checked="" type="checkbox"/> <input type="checkbox"/>
Mustermann Max (mmusterm) Information technology	<input type="checkbox"/> <input type="checkbox"/>

Sollte eine der beiden Aktionen ausgewählt worden sein, so können Sie die Maus über die Schaltfläche bewegen, um in einem Tooltip zu erfahren, zu welchem Zeitpunkt welche Person diese Entscheidung getroffen hat. Zusätzlich dazu finden Sie in allen Zeilen oder Spalten, die Personen darstellen, ein Personen-Icon. Durch einen Klick auf dieses Icon öffnet sich ein Dialog, in welchem die Stammdaten der betroffenen Person angezeigt werden.

Sollten mehr als 5 Spalten angezeigt werden, wird oberhalb der Tabelle ein Paginator angezeigt, mit welchem Sie durch die Spalten navigieren und auch verändern können, wie viele Spalten angezeigt werden.

Da die Rezertifizierungsmatrix, je nach Kategorie, unterschiedlich aufgebaut ist, wird immer nur eine Kategorie angezeigt, auch wenn in der Richtlinie mehrere Kategorien eingerichtet wurden. Im Bereich "Kategorien" können Sie zwischen den einzelnen Kategorien der Rezertifizierung wechseln. Im Bereich "Filter" können Sie die Matrix nach bestimmten Kriterien filtern.

Filter	Beschreibung
Status	<p>Diese Einstellung filtert nach dem Status der jeweiligen Rezertifizierung. Folgende Auswahlmöglichkeiten stehen zur Verfügung:</p> <ul style="list-style-type: none"> • *: Alle Rezertifizierungen werden angezeigt. • Offen: Nur Rezertifizierungen, welche noch nicht ausgewählt wurden, werden angezeigt. • Rezertifiziert: Nur bestätigte Rezertifizierungen werden angezeigt. • Nicht Rezertifiziert: Nur Rezertifizierungen, die abgelehnt (nicht rezertifiziert) wurden, werden angezeigt. • Deaktiviert: Nur Rezertifizierungen, die nicht rezertifiziert werden können, da Sie aus automatischen Profilzuordnungen resultieren, werden angezeigt.
Abteilung	<p>Filtert die Matrix nach allen Zeilen/Spalten, in welchen die Rezertifizierung für eine Person der gewählten Abteilung ist.</p>
Ressource	<p>Lässt die Matrix nach bestimmten tenfold-Ressourcen filtern. Dieser Filter steht nur für die Kategorien "Ressourcen" und "Anwendungsberechtigungen" zur Verfügung.</p>

Filter	Beschreibung
Nur Zeilen mit sichtbaren Rezertifizierungen anzeigen	Mit diesem Filter lassen sich alle Zeilen ausblenden, in denen nur Rezertifizierungen in gerade nicht dargestellten Spalten zu finden sind.

Meine Rezertifizierungen

Mit der Systemberechtigung "View My Recertifications" (8313) erhalten Benutzer, über die Kachel "Meine Rezertifizierungen" im Startbereich, Zugang zu einer Abwandlung dieser Maske, wo sie nur Rezertifizierungen aufgelistet finden, für die sie selbst zuständig sind oder waren.

11.2.2 Rezertifizierungen durchführen

Für jede Richtlinie, für die eine Person als Zertifizierer bestimmt wurde und für welche es offene Rezertifizierungen gibt, erhält diese Person eine Kachel im Startbereich von tenfold, auf welcher angezeigt wird, wie viele offene Rezertifizierungen zu tätigen sind.

Durch einen Klick auf diese Kachel gelangen Sie auf die Maske zur Rezertifizierung. Diese ist genauso aufgebaut, wie die Übersichtsmaske aus dem vorhergehenden Abschnitt, zeigt jedoch nur die Rezertifizierungen an, für die Sie selbst zuständig sind. Außerdem können Sie hier über Buttons Rezertifizierungen bestätigen oder ablehnen.

tenfold

Ressourcen **Berechtigungen**

Rezertifizierung - M365 Gruppen
Im linken Menü kann die Kategorie ausgewählt werden, die rezertifiziert werden soll. Anschließend kann in der Tabelle festgelegt werden, welche Personen oder Berechtigungen noch korrekt und welche hingegen schon veraltet sind. [Zurück](#)

Kategorien
Microsoft 365-Gruppen

Rezertifizierung
Name: M365 Gruppen
Beschreibung:
Startdatum: 09.07.2021
Enddatum: 10.07.2021

Filter
Status: *
Abteilung: *
Nur Zeilen mit sichtbaren Rezertifizierungen anzeigen ☒

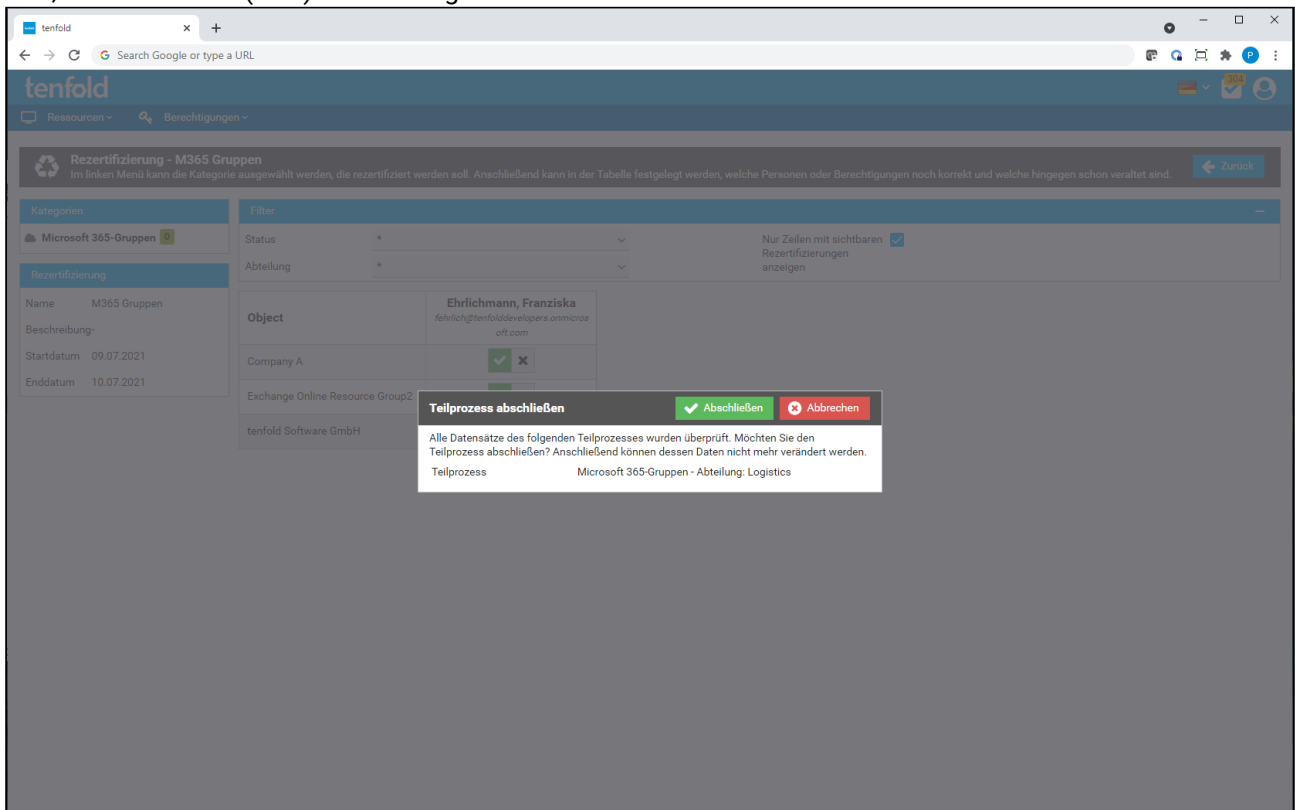
Objekt	Company A	Exchange Online Resource Group2
Ehrlichmann, Franziska f.ehrlichmann@tenfold.com, onmicrosoft.org	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
tenfold Software GmbH	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Für jeden Eintrag in der Matrix muss der zuständige Rezertifizierer entscheiden, ob die Rezertifizierung angenommen oder abgelehnt werden soll. Solange der Prozess noch offen ist, können Sie sich jederzeit umentscheiden oder, durch einen erneuten Klick auf die ausgewählte Option, die Auswahl wieder entfernen.

Sofortiges Speichern

Auch wenn die Rezertifizierung erst mit Abschluss des Prozesses durchgeführt wird, werden sämtliche Entscheidungen sofort abgespeichert. Sollten Sie die Maske also vorzeitig verlassen, sehen andere Personen in der Übersicht bereits getroffene Entscheidungen.

Sobald alle vorhandenen Rezertifizierungen abgeschlossen sind, öffnet sich ein Dialog, in welchem gefragt wird, ob der aktuelle (Teil-)Prozess abgeschlossen werden soll.



Wird hier die Schaltfläche "Abschließen" betätigt, so wird der (Teil-)Prozess abgeschlossen und weitere Änderungen sind nicht mehr möglich. Je nach den Einstellungen in der Richtlinie, werden die nötigen Löschvorgänge und Genehmigungsworkflows nun durchgeführt, oder es wird auf weitere Teilprozesse oder eine bestimmte Uhrzeit gewartet.

Wenn Sie die Schaltfläche "Abbrechen" betätigen, so bleibt der Prozess weiterhin offen und Änderungen sind nach wie vor möglich. Wenn Sie zu einem späteren Zeitpunkt den Prozess abschließen möchten, können Sie die Schaltfläche "Teilprozesse abschließen" verwenden, welche erscheint, wenn alle Entscheidungen getroffen sind, der Prozess jedoch noch offen ist. Wenn Sie eine Entscheidung abwählen, verschwindet die Schaltfläche wieder. Werden danach wieder alle möglichen Entscheidungen ausgewählt, erscheint erneut der Dialog "Teilprozess abschließen".

Für alle akzeptierten Rezertifizierungen bleiben die Objektzuordnungen erhalten, ohne dass seitens tenfold eine Aktion ausgelöst wird.

12 Einstellungen

12.1 Application Server

12.1.1 RAM-Einstellungen

Bedeutung

Der tenfold Applikationsserver läuft innerhalb einer Java Virtual Machine (JVM). Beim Start der JVM werden Option mitgegeben, die angeben, wie viel Hauptspeicher (RAM) die JVM maximal verbrauchen darf. Die aktuelle Standardeinstellung für tenfold beträgt 4096 MB.

Ändern der Einstellung

Es wird allerdings für optimale Performance empfohlen, diesen Wert auf mindestens 8192 MB zu erhöhen. Dazu gehen Sie folgendermaßen vor:

- Stoppen Sie den Dienst "tenfold Server"
- Öffnen Sie die Konfigurationsdatei standalone.conf.bat (diese befindet sich unter <tenfold>\server\bin\) in einem Editor
- Suchen Sie nach der Zeile, die mit "set "JAVA_OPTS=-Xms64M" beginnt
- In dieser Zeile ändern Sie den Parameter -Xmx von 4096M auf den gewünschten Wert (die Zahl nach "Xmx" gibt den RAM in Megabyte an; das abschließende "M" darf nicht ausgelassen werden!)
- Speichern Sie die Änderung
- Starten Sie den Dienst "tenfold Server"

Überprüfen der Einstellung

Sie können die neue Einstellung verifizieren, in dem Sie im Menü unter "Einstellungen" den Punkt "Systeminformationen" wählen. Dort finden Sie im Bereich "Hauptspeicher" den Eintrag "Maximaler Speicher". Dieser sollte dem in der Datei konfigurierten Wert abzüglich 0,5 - 1,5 GB (dies ist der Overhead der JVM selbst) betragen.

The screenshot shows the tenfold web application interface. The top navigation bar includes links for Personen, Ressourcen, Berechtigungen, Requests, Organisation, Workflows, Provisioning, and Einstellungen. The main content area is titled 'Systeminformationen' and displays various system details.

Systeminformationen	
tenfold-Version	tenfold 18.1.2 r7763
tenfold-Speicherort	C:\tenfold\server\bin\
Java Version	1.8.0_144
JSF-Version	2.2.16
PrimeFaces-Version	6.1
Hibernate Version	5.0.10.Final
Groovy Version	2.4.14

Datenbank	
Produkt	Microsoft SQL Server
Version	14.00.1000

Hauptspeicher	
Maximaler Speicher	3641 MB
Freier Speicher	2262 MB
Verwendeter Speicher	37%
Garbage Collector	Garbage Collector starten

Logging Einstellungen	
Skript Ausgabe	<input checked="" type="checkbox"/>
JSF Phase Logging	<input type="checkbox"/>

Cache		
EXEC cache	Ausgabe in Logdatei	Cache leeren
Hibernate cache	Ausgabe in Logdatei	Cache leeren
Person picture cache	Ausgabe in Logdatei	Cache leeren
Resource picture cache	Ausgabe in Logdatei	Cache leeren
Field rule cache	Ausgabe in Logdatei	Cache leeren
Field rule assignment cache	Ausgabe in Logdatei	Cache leeren
Related department cache	Ausgabe in Logdatei	Cache leeren
Related office cache	Ausgabe in Logdatei	Cache leeren
Plugin caches	Ausgabe in Logdatei	Caches leeren
Field mapping caches	Ausgabe in Logdatei	Caches leeren

Troubleshooting

Sollte die JVM keinen zusätzlichen Hauptspeicher mehr zur Verfügung haben, kann es dazu kommen, dass tenfold nicht mehr erreichbar ist bzw. auf Klicks nicht mehr reagiert. In diesem Fall erhöhen Sie, entsprechend der Anleitung oberhalb, den Hauptspeicher von **4 auf 8 GB** bzw. von **8 auf 16 GB oder mehr**.

Häufig tritt dieses Problem auf, wenn eine sehr hohe Anzahl an Verzeichnissen auf einem Fileserver im Rahmen eines Scan verarbeitet werden müssen.

12.1.2 Datenbankverbindung

Die Einstellungen für die Verbindung vom Application Server zur Datenbank können nicht über die tenfold-Oberfläche gemacht werden. Der tenfold Dienst kann nur erfolgreich gestartet werden, wenn eine gültige Datenbankverbindung existiert. Die Datenbankverbindung wird im Rahmen der Softwareinstallation im Installationsassistenten eingegeben. Wenn die Daten zur Verbindung nachträglich geändert werden müssen, so muss dies manuell in der Konfigurationsdatei durchgeführt werden.

Änderungen

1. Passen Sie die Konfiguration an (siehe unten)
2. Starten Sie den tenfold Server-Dienst erneut
3. Prüfen Sie, ob die Verbindung funktioniert

Anpassung der Verbindung

Um die Verbindung anzupassen, öffnen Sie die Konfigurationsdatei. Diese befindet sich im Installationsverzeichnis (Standard ist C:\tenfold\)\ im Unterverzeichnis "server\standalone\configuration" und besitzt den Namen standalone.xml. Navigieren Sie zu nachfolgender Stelle in der Datei.

Microsoft SQL Server Beispiel:

```
<datasource jndi-name="java:/tenfoldDS" pool-name="tenfoldDS" enabled="true" use-java-context="true">
  <connection-url>jdbc:sqlserver://
localhost\SQLEXPRESS:1433;databaseName=tenfold;integratedSecurity=true</connection-url>
  <driver>driver.mssql</driver>
  <security>
    <user-name>tenfold\service-sql-user</user-name>
    <password><![CDATA[ZZZZ]]></password>
  </security>
```

Oracle Beispiel:

```
<datasource jndi-name="java:/tenfoldDS" pool-name="tenfoldDS" enabled="true" use-java-context="true">
  <connection-url>jdbc:oracle:thin:@localhost:1522/tenfold</connection-url>
  <driver>driver.oracle</driver>
  <security>
    <user-name>ora-tenfold-sql</user-name>
    <password><![CDATA[YYYY]]></password>
  </security>
```

Connection URL

Im Tag <connection-url> wird der Datenbanktyp, der Hostname und Port sowie herstellerspezifische Optionen angegeben.

Der Aufbau für SQL Server ist folgender:

1. Am Beginn steht "jdbc:sqlserver://".
2. Anschließend folgt der Hostname des Datenbankservers, im Beispiel lautet dieser "localhost"
3. Es folgt anschließend der Instanzname der Datenbank, gefolgt von einem Doppelpunkt und dem TCP-Port
4. Anschließend folgt der Name der Datenbank, getrennt von einem Strichpunkt.
5. Die Einstellung "integratedSecurity" wird auf true gesetzt, wenn für die Verbindung ein Domain-Benutzer verwendet wird. Wenn ein reiner SQL-Benutzer verwendet wird, ist die Einstellung auf false zu setzen.

Der Aufbau für Oracle ist folgender:

1. Am Beginn steht "jdbc:oracle:thin:"
2. Es folgt ein "@" Zeichen, gefolgt vom Hostnamen, einem Doppelpunkt und dem TCP-Port
3. Schließlich folgt ein Schrägstrich gefolgt vom Namen des Datenbankschemas

Driver

Die Einstellung wählt den Datenbanktreiber aus. Sie ist für SQL-Server auf "driver.mssql" zu stellen. Für Oracle muss "driver.oracle" verwendet werden.

Security

Im Bereich Security werden die Anmeldeinformationen übergeben. Folgende Einstellungen sind zu wählen:

Datenbank	Einstellung	SSO	Wert
Microsoft SQL Server	user-name	Ja	Den Benutzernamen inklusive Domain im Format <i>DOMAIN\username</i>
Microsoft SQL Server	user-name	Nein	Den SQL-Benutzernamen
Microsoft SQL Server	password	Ja	Bei SSO wird das Password ignoriert. Die Einstellung muss jedoch vorhanden sein. Setzen Sie den Wert deshalb auf einen Dummywert wie <code><![CDATA[ZZZ]]></code>
Microsoft SQL Server	password	Nein	Das Password des SQL-Benutzers im Klartext innerhalb eines CDATA-Elements (aufgrund möglicher Sonderzeichen) Beispielsweise: <code><![CDATA[p@assword]]></code>
Oracle Database	user-name	n/a	Der Oracle-Benutzername
Oracle Database	password	n/a	Das Password des Oracle-Benutzers im Klartext innerhalb eines CDATA-Elements (aufgrund möglicher Sonderzeichen) Beispielsweise: <code><![CDATA[p@assword]]></code>

Sicherheit - Sehr wichtige Hinweise

Wählen Sie für den Datenbankbenutzer unbedingt ein gutes Password. Sollten die Anmeldungsinformationen in falsche Hände geraten, so ist dem Angreifer der Zugriff und die Manipulation aller Daten in der tenfold-Datenbank möglich. Wenn Sie einen SQL-Server mit SQL-Benutzer oder Oracle verwenden, stellen Sie unbedingt sicher, dass der Dateisystemzugriff auf die Datei "standalone.xml" nur für den Administrator und den tenfold-Dienstbenutzer möglich ist, da sonst das Password, welches im Klartext angegeben werden muss, für unberechtigte Personen einsehbar sein könnte.

Troubleshooting

Wenn der tenfold Server-Dienst nach einer Anpassung nicht mehr erfolgreich startet, überprüfen Sie bitte das folgende:

- Ist der Benutzername richtig eingegeben?
- Für SQL Server-Benutzer und Oracle-Benutzer: Wurde das Password richtig hinterlegt? Wurde es in einem CDATA Element eingebettet?
- Für Active Directory-Benutzer: Wurde das password-Attribut mit einem in CDATA eingebetteten Dummy-Wert versehen?
- Ist der Treiber (Attribut "driver") korrekt eingestellt?

- Können Sie sich mit SQL Developer (Oracle) oder SQL Server Management Studio (für SQL Server) mit den jeweiligen Anmeldedaten an der tenfold-Datenbank anmelden und Befehle ausführen?

Art und Anzahl der Verbindungen

tenfold nutzt für die Verbindung zur Datenbank einen Pool-Service, der die Anzahl der individuellen Netzwerkverbindungen zum Datenbankserver eigenständig reguliert. Es werden dabei je nach Bedarf zwischen 1 und 20 Verbindungen aufgebaut. Die Verbindung erfolgt immer unter den in der Konfigurationsdatei im Bereich "security" angegebenen Benutzerdaten.

12.1.3 Einrichten von Single Sign On

Seit tenfold 2017 (17.1.1) hat sich die Konfiguration für die automatische Anmeldung von Benutzern an tenfold (Single Sign On / SSO) wesentlich vereinfacht.

Aktivierung bei einer neuen Installation

Wenn SSO in einer neuen tenfold Installation (nach Version 2017) aktiviert werden, soll, so muss nach der Systeminstallation lediglich der Systemparameter **"System.authentication.mode"** auf den Wert **"SSO"** gestellt werden.

Hinweis

Wie Systemparameter angezeigt und geändert werden, wird in [Systemparameter\(see page 484\)](#) beschrieben.

Aktualisierung der Einstellungen bei bestehenden Installationen

Soll eine bestehende Installation auf tenfold 2017 migriert werden, so sind folgende Schritte erforderlich:

1. Aktualisierung des Applikationsservers auf die neue Version
2. Der Wert für den Systemparameter **"System.authentication.mode"** wird durch die Aktualisierung automatisch auf den Wert **"SETUP"** gestellt.
3. Öffnen Sie den Browser und wählen Sie die URL für den Applikationsserver an
4. Die Anmeldung erfolgt automatisch mit dem im Systemparameter **"System.authentication.setup.username"** hinterlegten Benutzer. (Üblicherweise muss dieser Wert vorab nicht angepasst werden)
5. Stellen Sie anschließend den Systemparameter auf den Wert **"SSO"** um
6. Schließen Sie alle Browserfenster, öffnen Sie den Browser erneut und wählen Sie die URL für den Applikationsserver an
7. Sie sollten nun erfolgreich mit Ihrem Benutzerkonto an tenfold angemeldet sein

Internet Explorer fragt nach Logindaten

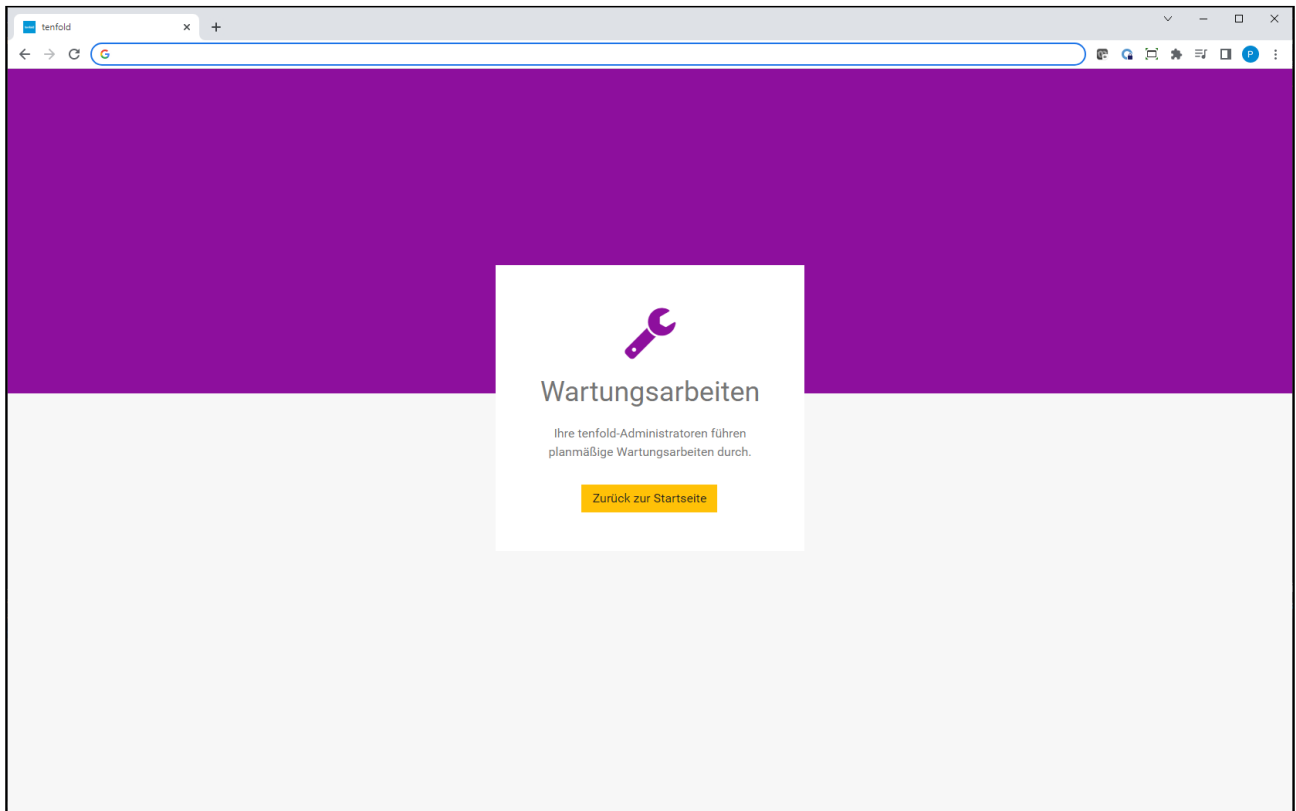
Läuft das tenfold-Service als Domänen-User, muss zusätzlich `setspn -s HTTP/<FQDN> <DOMAIN>\<USERNAME>` für den eingetragenen User ausgeführt werden.

Dieser Befehl muss einmal für den kurzen und einmal für den langen Namen ausgeführt werden:

- `setspn -s HTTP/serverName <DOMAIN>\<USERNAME>`
- `setspn -s HTTP/serverName.domainname.local <DOMAIN>\<USERNAME>`

Danach kann es einige Zeit dauern bis die Änderung überall aktiv sind.

12.2 Wartungsmodus

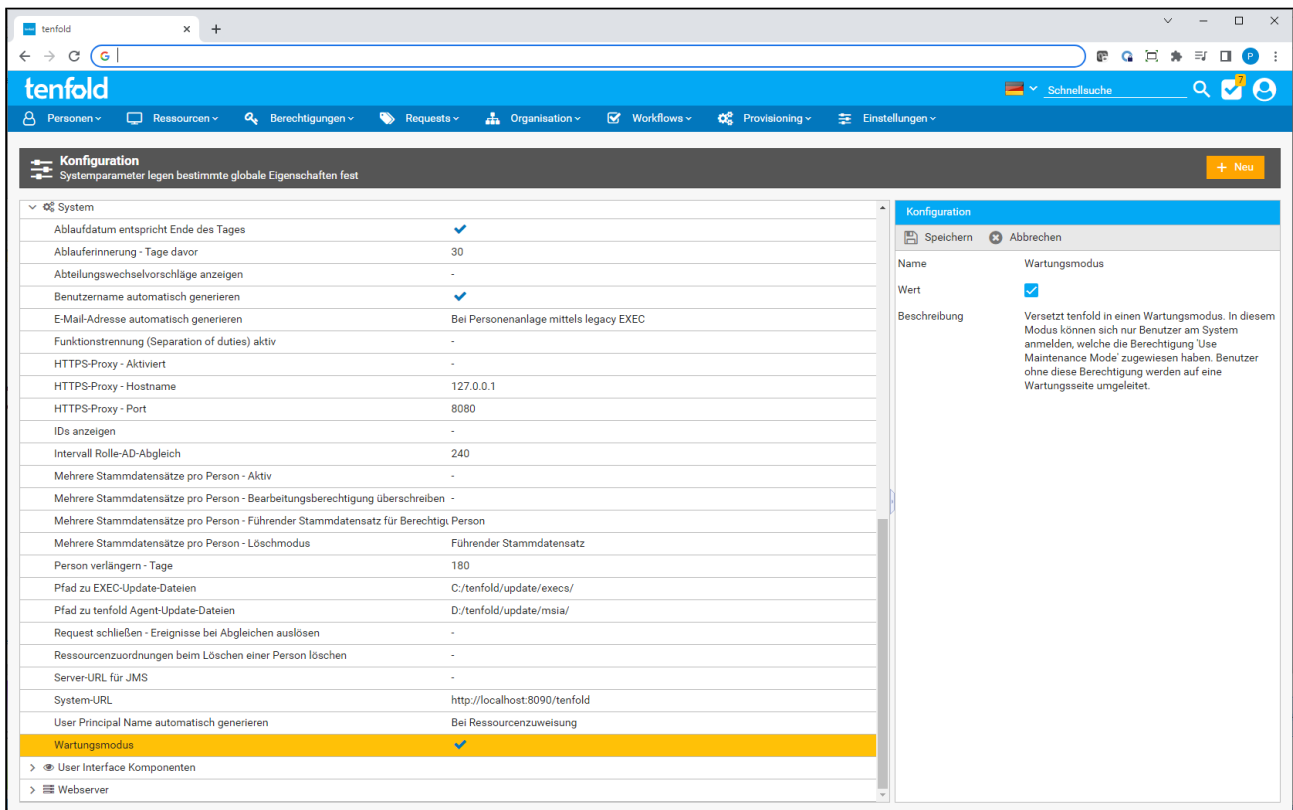


(see page 521)

Oftmals ist es während der Einrichtung neuer Funktionen von tenfold notwendig, Konfigurationen vorzunehmen, welche über mehrere Masken verteilt sind und eine längere Zeit in Anspruch nehmen können. Wenn während dieser Zeit Benutzer mit tenfold arbeiten kann es dazu kommen, dass diese unvollständige oder fehlerhafte Ergebnisse aufgrund von unvollständigen Konfigurationen erhalten. Außerdem kann es passieren, dass während der Konfiguration Fehler gemacht werden. Deshalb wäre es gut, diese ungestört zu testen, bevor die Anwender mit den neuen Funktionen arbeiten sollen.

Zu diesem Zweck bietet Ihnen tenfold einen Wartungsmodus, welcher nur Anmeldungen einer eingeschränkten Anwendergruppe zulässt.

Um tenfold in den Wartungsmodus zu schalten, öffnen Sie Maske der Systemparameter, erreichbar im Menü unter *Einstellungen* > *System* > *Parameter*. Machen Sie dort die Einstellung *System* > *Wartungsmodus* ausfindig und haken die Einstellung an. Betätigen Sie nun die Schaltfläche "Speichern", um den Wartungsmodus zu aktivieren.



Sobald der Wartungsmodus aktiv ist können sich nur noch Personen mit der Berechtigung "Use Maintenance Mode" (9120) an tenfold anmelden. Andere Benutzer erhalten eine entsprechende Meldung, dass sich tenfold im Wartungsmodus befindet und eine Anmeldung aktuell nicht möglich ist. Zur Erinnerung erscheint auf der Startseite von tenfold ebenso eine Nachricht für alle angemeldeten Benutzer auf, dass tenfold aktuell im Wartungsmodus ausgeführt wird.

Neustart

Da bereits angemeldete Benutzer weiterhin mit tenfold arbeiten können wird empfohlen tenfold nach Aktivierung des Wartungsmodus neu zu starten. Alternativ dazu können Sie auch die Sessions angemeldeter Benutzer beenden, um diese zu einer erneuten Anmeldung zu zwingen (siehe [Sessionverwaltung](#) (see page 521)). Dies empfiehlt sich dann, wenn nur wenige Benutzer am System angemeldet sind, um die Zeit eines Neustartes zu sparen.

12.3 Jobs

12.3.1 Allgemeines

tenfold verfügt über eine interne Job-Verwaltung. Diese ist dafür zuständig, periodisch wiederkehrende Tätigkeiten auszuführen. Beispiele hierfür sind:

- Abgleich mit dem Active Directory (um externe Änderungen zu erkennen)
- Abgleich mit den Fileservern (um externe Änderungen zu erkennen)
- Abgleich mit dem SAP (um externe Änderungen zu erkennen)
- Überprüfung von befristeten Berechtigungen/Benutzern (um diese automatisch zu löschen/deaktivieren)

Ein Job kann auf drei Arten gestartet werden:

- Cron-Auslöser: es handelt sich hierbei um einen zeitlichen Auslöser, der einen bestimmten Ausführungsplan hat (z.B. jeden Tag um 22:00, jeden ersten Montag im Monat, etc.)
- Dateiauslöser: der Job wartet auf Änderungen in einer bestimmten Datei und startet, sobald die Datei verändert wurde (dieser Auslöser wird für File Import/Export Schnittstellen verwendet. Er löst aus, sobald das exportierende System die Datei verändert hat, um die Daten anschließend in tenfold zu importieren)
- Manuelles auslösen: Jeder Job kann durch einen Administrator manuell gestartet werden

12.3.2 Verwaltung

Benötigte Berechtigung

Um die Job-Verwaltung durchzuführen, wird die Systemberechtigung "Job Administration" (8013) benötigt.

Die Verwaltung der Jobs ist über das Menü erreichbar: Einstellungen > Jobs > Verwaltung.

Im Rahmen des Customizing können neue Jobs zum System hinzugefügt werden. Das ist insbesondere dann notwendig, wenn tenfold sich mit den Benutzer- und Berechtigungsdatenbanken von anderen Applikationen synchronisieren soll.

Editionen

In der Essentials Edition und Essentials Edition Plus ist das Hinzufügen neuer Jobs nicht möglich. Es können lediglich die Einstellungen der bestehenden Jobs angepasst werden.

Spezielle Jobs

Es gibt spezielle Jobs, welche nicht ohne Kontaktaufnahme mit dem Support verändert werden sollten (mit Ausnahme der zeitlichen Planung über den Cron-Auslöser):

- Active Directory Group Expiry Date Check (überprüft das Ablaufdatum von Active Directory Berechtigungen und entfernt diese gegebenenfalls)
- Active Directory Object Sync (synchronisiert Benutzer, Gruppen und andere Active Directory Objekte mit tenfold)
- Active Directory Personen Sync (synchronisiert Benutzer aus dem Active Directory und legt Personen in tenfold für die jeweiligen Benutzer an)
- Active Directory Picture Sync (synchronisiert die Bilddaten, die in Active Directory hinterlegt sind)
- Scheduled Request Trigger (überprüft periodisch, ob es geplante Requests gibt, welche nunmehr ausgeführt werden müssen)
- Share Sync (synchronisiert Verzeichnisstruktur und ACLs der hinterlegten Freigaben mit tenfold)

Liste der Jobs

Auf der Maske "Jobs" (Einstellungen > Jobs > Verwaltung) werden alle im System befindlichen Jobs aufgelistet. Folgende Informationen werden dabei angezeigt:

- Name: die Bezeichnung des Jobs
- Typ: Gibt an, ob es sich um einen zeitgesteuerten oder einen dateigesteuerten Job handelt

- Cron-Auslöser: Gibt im Falle eines zeitgesteuerten Jobs den hinterlegten Cron-Auslöser an (für dateigesteuerte Jobs ist dieser Wert immer leer)
- Dateiauslöser: Gibt im Falle eines dateigesteuerten Jobs den hinterlegten lokalen oder UNC-Pfad für die zu überwachende Datei an (für zeitgesteuerte Jobs ist dieser Wert immer leer)
- Nächste Durchführung: Gibt im Falle von zeitgesteuerten Jobs den nächsten planmäßigen Durchführungszeitpunkt an (für dateigesteuerte Jobs ist dieser Wert immer leer)

Job-Einstellungen bearbeiten

Um die Einstellungen für einen Job zu bearbeiten, wählen Sie im Kontextmenü des jeweiligen Eintrags die Aktion "Bearbeiten".

Es können anschließend folgende Einstellungen getroffen werden:

Einstellung	Beschreibung	Beispielwert
Name	Legt die Bezeichnung des Jobs fest. Diese dient lediglich der Darstellung innerhalb von tenfold.	My new job
Typ	Bei der Anlage eines Job wird festgelegt, ob es sich um einen zeitgesteuerten (Cron-Auslöser) oder dateigesteuerten (Dateiauslöser) Job handelt. Diese Einstellung kann im Nachhinein nicht mehr geändert werden, und wird lediglich zur Information angezeigt.	
Cron-Auslöser (nur bei zeitgesteuerten Jobs)	Hier wird im Cron-Format festgelegt, zu welchen Zeitpunkten der Jobs gestartet werden soll. Zur Erläuterung des Cron-Formats siehe https://www.quartz-scheduler.org/documentation/quartz-2.3.0/tutorials/tutorial-lesson-06.html	0 0 22 ? * * (bedeutet jeden Tag um 22:00)
Dateiauslöser (nur bei dateigesteuerten Jobs)	Es wird der Pfad zur Datei festgelegt, welche überwacht werden soll. Es werden sowohl lokale Dateien auf dem tenfold Server, als auch Dateien auf anderen Rechnern (via UNC-Pfad) unterstützt.	C:/mydir/ myfile.csv \\srv1- fs\mydir\myfile.cs v
EXEC	Legt fest, welcher EXEC für die Bearbeitung des Jobs vorgesehen ist.	
Aktiv	Hier kann festgelegt werden, ob der Job aktiv ist oder nicht. Wird ein Job deaktiviert, so wird der entsprechende EXEC nicht ausgeführt, auch wenn der Cron- oder Dateiauslöser auslöst.	

Im Karteireiter "Selected Workflow" sehen Sie den Quellcode des EXEC, welcher für den aktuellen Job vorgesehen ist.

Cron-Auslöser Beispiele

Die folgenden Beispiele zeigen die Verwendung der Cron-Auslöser Syntax.

Cron-Auslöser	Bedeutung
0 0 22 * * ?	Der Job startet jeden Tag genau um 22 Uhr.
0 15 16 * * ?	Der Job startet jeden Tag genau um 16:15 Uhr
0 0 1/1 * * ?	Der Job startet zum ersten Mal um 1 Uhr und ab dann jede weitere Stunde.
0 0 18-22 * * ?	Der Job startet zum ersten Mal um 18 Uhr und ab dann jede weitere Stunde bis 22 Uhr.
0 15 10 ? * MON-FRI	Der Job startet Montag bis Freitag jeweils um 10:15 Uhr

Job löschen

Um einen Job vom System zu entfernen, klicken Sie im Kontextmenü des gewünschten Eintrags auf die Aktion "Löschen". Sie werden aufgefordert die Löschung zu bestätigen.

Löschen

Achtung: Es gibt keine Möglichkeit einen gelöschten Job mit Standardmethoden wiederherzustellen.

Job ausführen

Es kann manchmal notwendig sein, einen bestimmten Job sofort auszuführen und nicht auf den nächste reguläre Ausführungszeitpunkt zu warten. Um dies zu bewerkstelligen, wählen Sie im Kontextmenü des Jobs, den Sie starten wollen die Aktion "Jetzt ausführen".

Ausführung abbrechen

Falls ein Job, welcher aktuell läuft abgebrochen werden muss, so ist dies über die Maske "Historie" möglich. Stellen Sie die Filtereinstellungen auf folgende Werte ein:

- Start/Ende: Wählen Sie den heutigen Tag aus
- Status: Laufend

Klicken Sie anschließend auf die Schaltfläche "Aktualisieren" und wählen Sie im Kontextmenü für den gewünschten Eintrag die Aktion "Abbrechen".

Es öffnet sich anschließend ein Dialog, auf welchem Sie entscheiden können, ob ein Rollback erforderlich ist, bevor der Job abgebrochen wird. Wird die Option gewählt so bedeutet das, dass tenfold die laufende Datenbank-Transaktion abbricht und zurückrollt. Etwaige Datenänderungen die im Laufe der Verarbeitung durchgeführt wurden, werden damit wieder auf den Ursprungszustand zurückgesetzt.

Transaktionen

Die Option für den Rollback greift nur, wenn der zugrundeliegende EXEC keine manuelle Transaktionssteuerung anwendet. Die meisten EXECs für Synchronisierungsvorgänge nutzen aus Performancegründen eine manuelle (dem EXEC obliegende) Transaktionssteuerung für die tenfold Datenbank. Bei diesen Jobs hat das Setzen der Option "Rollback erforderlich" keine Auswirkung.

12.3.3 Historie

Jede Ausführung eines Jobs wird aus Gründen der Nachvollziehbarkeit innerhalb von tenfold protokolliert. Das Protokoll kann über eine entsprechende Funktion eingesehen werden, welche unter Einstellungen > Jobs > Historie erreichbar ist.

Benötigte Berechtigung

Um die Job-Historie einsehen zu können, wird die Systemberechtigung "Job History Administration" (8014) benötigt.

Die Anzeige der Einträge in der Historie kann über einige Filter gesteuert werden:

- **Start/Ende:** definiert das Zeitfenster, aus welchem Einträge angezeigt werden sollen
- **Name:** Hier kann ein Teil eines Jobnamens eingegeben werden. Es werden nur Jobs, deren Namen auf den Filter passen angezeigt.
- **Status:** Ermöglicht die Einschränkung auf Basis des Job-Status

Stellen Sie die gewünschten Filter ein und klicken Sie auf die Schaltfläche "Aktualisieren".

Für jeden Eintrag werden Informationen angezeigt:

- **Start:** Der Zeitpunkt, an dem der Job gestartet wurde
- **Name:** Gibt an, auf welchen Job sich der Eintrag bezieht
- **Fortschritt:** Zeigt bei laufenden Jobs den Fortschritt in der Verarbeitung an.
- **Ende:** Sofern der Job im Status "Abgeschlossen" oder "Fehlgeschlagen" ist, wird hier der Endzeitpunkt der Verarbeitung angezeigt
- **Laufzeit:** Gibt die gesamte Laufzeit in Stunden, Minuten und Sekunden an (echte Laufzeit, keine CPU-Zeit oder ähnliches)
- **Status:** Gibt den Status des Eintrags an

Fortschrittsanzeige

Entweder erfolgt eine Anzeige in Prozent (wenn der zugrundeliegende EXEC dies unterstützt) oder es wird lediglich ein Hinweis angezeigt.

Jeder Eintrag kann sich in einem bestimmten Status befinden, welche nachfolgend beschrieben werden:

- **Abgebrochen:** der Job wurde durch den Administrator explizit abgebrochen
- **Abgeschlossen:** der Job wurde ohne Fehlermeldung beendet
- **Fehlgeschlagen:** es ist während der Ausführung ein schwerwiegender Fehler aufgetreten, welcher die weitere Verarbeitung unmöglich gemacht hat
- **Laufend:** der Job läuft in diesem Moment
- **Nicht ausgeführt:** der Cron-Auslöser für den Job wurde ausgelöst, aber der Job läuft zu diesem Zeitpunkt bereits.

Status "Nicht ausgeführt"

Wenn ein Eintrag den Status "nicht ausgeführt" aufweist, dann bedeutet dies, dass der Cron-Auslöser des Jobs ausgelöst wurde, während der Job noch aktiv war. Das kann auftreten, wenn ein Job so lange läuft, dass er sich über den Cron-Auslöser selbst überholt. In diesem Fall wird der Job nicht nochmals gestartet (jeder Job darf nur einmal gleichzeitig aktiv sein). Zur Dokumentation wird jedoch ein Eintrag in der Job-Historie angelegt.

Detaillierte Informationen zu Scans

Detailliertere Informationen zu Jobs, welche Synchronisationen mit Fileservern, Exchange® und SharePoint® ausführen, befinden sich darüber hinaus auf der Maske "Scans". Siehe dazu auch: Scan-Historie

12.4 Benachrichtigungen

Während des Betriebs von tenfold laufen die verschiedensten Prozesse sowohl im Hintergrund ab als auch ausgelöst durch Benutzeraktionen. Oftmals kann es dabei vorkommen, dass ein Eingreifen innerhalb oder außerhalb von tenfold notwendig ist. Wenn zum Beispiel ein Job regelmäßig fehlschlägt, kann es sein, dass Einstellungen angepasst werden müssen. Wenn ein Request lange Zeit ungenehmigt bleibt, müssen möglicherweise die Genehmiger kontaktiert werden. Für solche Fälle können in tenfold Benachrichtigungen hinterlegt werden, um zeitnah Informationen über Missstände und andere Ereignisse zu erhalten, die ein Eingreifen erforderlich machen.

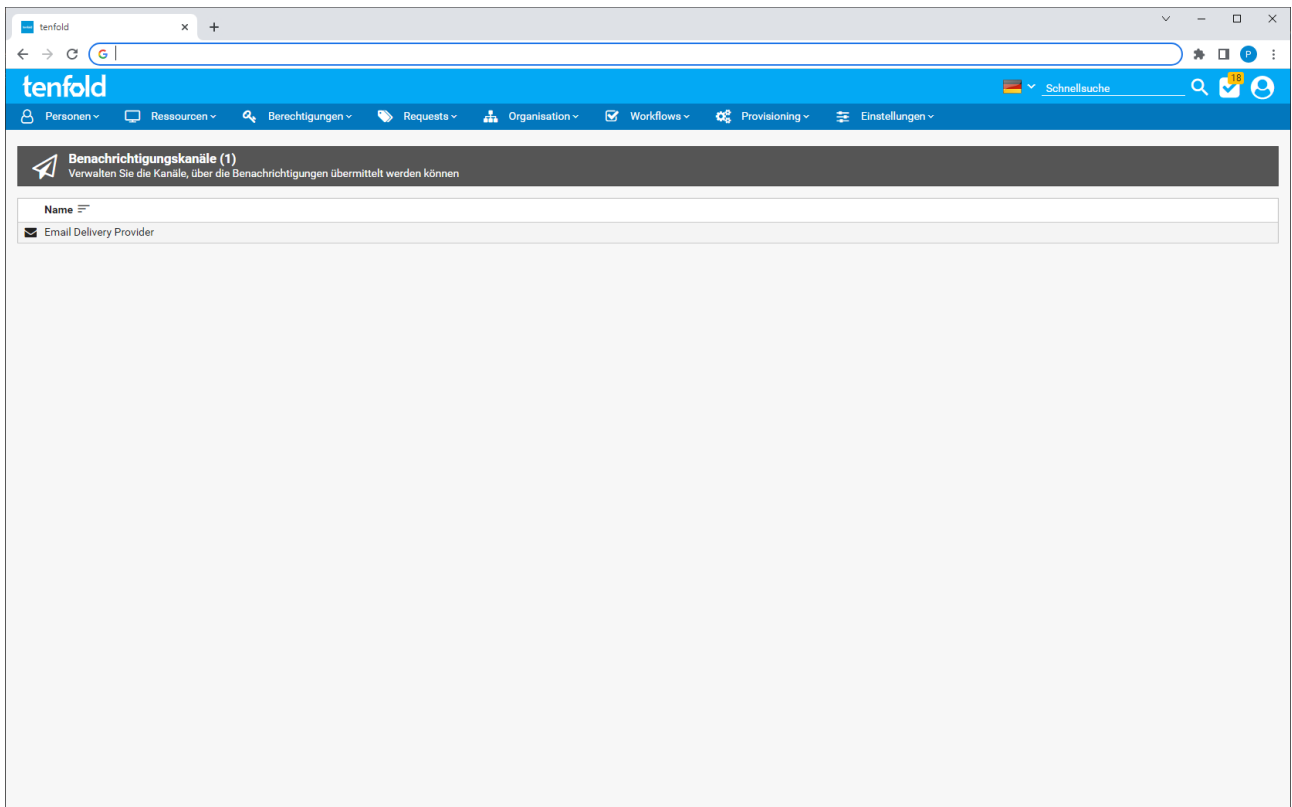
Hierfür können Benachrichtigungen über verschiedenste Kanäle (z.B. E-Mail- oder Ticketsysteme) versendet werden, um nicht ständig Übersichtsmasken in tenfold prüfen zu müssen. Darüber hinaus enthalten Benachrichtigungen einen Status, welcher anzeigt, in welchem Verarbeitungszustand sich die Benachrichtigung befindet. Dies ist vor allem dann hilfreich, wenn mehrere Personen dafür verantwortlich sind, dieselbe Benachrichtigung zu prüfen.

In folgenden Status kann sich eine Benachrichtigung befinden:

Status	Beschreibung
Offen	Die Benachrichtigung wurde versendet, jedoch noch nicht bearbeitet.
Bestätigt	Die Benachrichtigung wurde fertig bearbeitet.
Fehlgeschlagen	Beim Versenden der Benachrichtigung trat ein Fehler auf.

12.4.1 Kanäle

Bei Benachrichtigungskanälen handelt es sich um Methoden, mit welchen tenfold die Benachrichtigungen versendet.



Benötigte Berechtigung

Für die Verwaltung ist die Berechtigung "Manage Alert Delivery Modes" (9203) erforderlich.

Über den Menüpunkt *Einstellungen* > *Benachrichtigungen* > *Kanäle* gelangen Sie zur Wartungsmaske der Benachrichtigungskanäle. Sie finden dort eine Auflistung sämtlicher vorhandener Kanäle. Mittels der Schaltfläche "Neu" im Kopfbereich der Maske können Sie einen neuen Kanal erstellen. Im Aktionsmenü der jeweiligen Kanäle können Sie bestehende Kanäle mit der Aktion "Löschen" wieder entfernen oder deren Einstellungen mit der Aktion "Bearbeiten" ändern. Standardmäßig wird tenfold mit dem Kanal "Email Delivery Provider" ausgeliefert, welcher vom Typ "E-Mail" ist. Dieser Kanal versendet Benachrichtigungen als E-Mail mit dem in tenfold hinterlegten SMTP-Server (siehe [SMTP-Server](#)(see page 532)). Dieser Kanal enthält keine weiteren Einstellungen und kann nicht gelöscht werden. Auch lassen sich keine weiteren E-Mail-Kanäle anlegen.

Kanaltyp	Plugin	Beschreibung
E-Mail	-	Versendet Benachrichtigungen als E-Mail
Jira	Jira, 2.0+	Erstellt Benachrichtigungen als Tickets in einer Jira-Instanz.

Da sich die Einstellungsmöglichkeiten der jeweiligen Kanäle stark unterscheiden, werden die Einstellungen in der Beschreibung des jeweiligen Plugins behandelt, welches den Kanaltyp mitliefert.

12.4.2 Verwaltung

Nachdem Sie die Kanäle zum Versenden von Benachrichtigungen definiert haben, können diese verwendet werden, um Benachrichtigungen zu versenden. Für diese Einstellungen navigieren Sie im Menü zu *Einstellungen > Benachrichtigungen > Verwaltung*.

Benötigte Berechtigung

Für die Verwaltung ist die Berechtigung "Manage Alert Subscriptions" (9202) erforderlich.

Zu Beginn finden Sie eine Tabelle mit allen konfigurierten Benachrichtigungen vor. Sie können die Anzeige im Bereich "Filter" nach Typ, Name und Status der Benachrichtigungen filtern. Nach der Installation von tenfold finden Sie folgende Benachrichtigungen vor, welche automatisch konfiguriert wurden:

Benachrichtigung	Beschreibung
Job could not start	Diese Benachrichtigung wird immer ausgelöst, wenn ein Job nicht gestartet werden konnte. Dies geschieht normalerweise dann, wenn ein Job noch läuft, während versucht wurde, ihn wieder zu starten (jeder Job kann nur einmal zur gleichen Zeit aktiv sein, siehe Jobs (see page 443)).
Job failed	Diese Benachrichtigung wird ausgelöst, wenn bei der Durchführung eines Jobs ein Fehler auftritt.
License audit	Diese Benachrichtigung wird jeden Tag ausgelöst, wenn die Anzahl der freien tenfold-Lizenzen unter einen konfigurierbaren Prozentsatz fällt.

Benachrichtigung	Beschreibung
System message	Hierbei handelt es sich um eine Sammelbenachrichtigung, welche für verschiedene wichtige Informationen verwendet wird.

Diese Benachrichtigungen können nicht entfernt werden, aber es können weitere Benachrichtigungen dieser Typen erstellt werden, deren Einstellungen Sie bearbeiten können.

Um eine neue Benachrichtigung hinzuzufügen, betätigen Sie die Schaltfläche "Neu" im Kopfbereich der Maske. Es erscheint ein Dialog, in welchem Sie den Benachrichtigungstyp auswählen können. Wählen Sie den gewünschten Typ und klicken auf die Schaltfläche "Weiter", um zur Konfiguration der Benachrichtigung zu gelangen. Wenn Sie mit den Einstellungen fertig sind, klicken Sie auf die Schaltfläche "Speichern", um die Anlage der neuen Benachrichtigung abzuschließen.

Folgende weitere Benachrichtigungen können hinzugefügt werden:

Benachrichtigung	Plugin	Beschreibung
Ausstehende Requests	-	Diese Benachrichtigung wird ausgelöst, wenn ein Request eine bestimmte Anzahl an Tagen ungenehmigt bleibt.

Plugins

Einige Benachrichtigungen stehen erst mit der Installation von Plugins zur Verfügung. Das Plugin und die notwendige Version können Sie der obigen Tabelle entnehmen. Weitere Details zu diesen Benachrichtigungen entnehmen Sie den Kapiteln zu den jeweiligen Plugins.

Allgemeine Einstellungen

Unabhängig von ihrem Typ verfügt jede Benachrichtigung über folgende Einstellungen:

Einstellung	Beschreibung
Name	Der Name der Benachrichtigung. Dieser wird zur Anzeige in der Liste verwendet.
Verantwortlich	Definiert die Personengruppe, welche die Benachrichtigung erhält. Sie haben folgende Auswahlmöglichkeiten: <ul style="list-style-type: none"> • Administratoren: Die Benachrichtigung wird an alle Mitglieder der tenfold-Rolle "Administratoren" gesendet. • Berechtigung: Die Benachrichtigung wird an alle Personen gesendet, welche über eine frei wählbare Berechtigung in tenfold verfügen.
Berechtigung	Wurde in der Einstellung "Verantwortlich" die Auswahl "Berechtigung" getroffen, so kann hier die erforderliche Berechtigung eingestellt werden.

Darüber hinaus kann eingestellt werden, über welche definierten Kanäle eine Benachrichtigung versandt werden soll. Um einen neuen Kanal hinzuzufügen, betätigen Sie die Schaltfläche "Neu" im Bereich "Kanäle". Es erscheint daraufhin ein Dialog, in welchem Sie einen Kanal zum Hinzufügen auswählen können. Je nach Kanal können hier zusätzliche Einstellungen getroffen werden:

Einstellung	Beschreibung
E-Mail	
Zusätzliche Empfänger	Eine kommasetrennte Liste weiterer E-Mail-Adressen, an welche die Benachrichtigung verschickt werden soll. Hinweis: Inhaber dieser E-Mail-Adressen erhalten nicht automatisch die Berechtigungen in tenfold, um Benachrichtigungen zu bearbeiten.
Vorlageneinstellung	Definiert, ob die Standardvorlage oder eine benutzerdefinierte Vorlage für die E-Mail-Nachricht verwendet werden soll.
Vorlage	Bestimmt die Vorlage, welche zur Erzeugung der E-Mail-Nachricht verwendet wird. Dieses Feld wird nur angezeigt, wenn in der Einstellung "Vorlageneinstellung" die Auswahl "Selbsterstellte Vorlage verwenden" ausgewählt wurde.

Die Einstellungen für Kanaltypen, die von Plugins geliefert werden, werden in den Kapiteln des jeweiligen Plugins näher beschrieben.

Mittels der Aktion "Bearbeiten" im Aktionsmenü des jeweiligen Kanals können Sie den Dialog erneut öffnen, um die Einstellungen zu ändern. Mit der Aktion "Löschen" können Sie den Versand einer Nachricht über diesen Kanal wieder entfernen.

Keine Kanäle

Es ist möglich, alle Kanäle einer Benachrichtigung zu entfernen. Damit werden die Benachrichtigungen nur noch in tenfold angezeigt. Dies wird **nicht** empfohlen, da damit die verantwortlichen Personen regelmäßig tenfold auf offene Benachrichtigungen prüfen müssen.

Die einzelnen Benachrichtigungen verfügen darüber hinaus über weitere individuelle Einstellungsmöglichkeiten:

Einstellung	Beschreibung
Job konnte nicht gestartet werden	
Priorität	Legt die Priorität fest, mit welcher die Benachrichtigung angelegt wird. Diese wird zur Kategorisierung und Filterung von Benachrichtigungen in tenfold verwendet. Diese Einstellung kann für alle Jobs und für einzelne Jobs individuell festgelegt werden.
Kanäle	Legt fest, welche der oben eingestellten Kanäle zum Versand verwendet werden. Diese Einstellung kann für einzelne Jobs überschrieben werden.
Ausschließen	Mit dieser Einstellung können Sie einzelne Jobs von dieser Benachrichtigung ausschließen. Für diese Jobs wird dann weder eine Nachricht versandt noch eine Benachrichtigung in tenfold angelegt.
Job fehlgeschlagen	

Priorität	Legt die Priorität fest, mit welcher die Benachrichtigung angelegt wird. Diese wird zur Kategorisierung und Filterung von Benachrichtigungen in tenfold verwendet. Diese Einstellung kann für alle Jobs und für einzelne Jobs individuell festgelegt werden.
Kanäle	Legt fest, welche der oben eingestellten Kanäle zum Versand verwendet werden. Diese Einstellung kann für einzelne Jobs überschrieben werden.
Ausschließen	Mit dieser Einstellung können Sie einzelne Jobs von dieser Benachrichtigung ausschließen. Für diese Jobs wird dann weder eine Nachricht versandt noch eine Benachrichtigung in tenfold angelegt.
Lizenzaudit	
Prozentanteil der verfügbaren Lizenzen	Legt fest, ab welchem Prozentsatz der verfügbaren Lizenzen - gemessen an der Gesamtmenge lizenzierter Benutzer - täglich eine Benachrichtigung erstellt werden soll, sollte dieser Prozentsatz unterschritten werden. Sollten Sie 0% eintragen, so wird die Benachrichtigung nur erzeugt, wenn alle verfügbaren Lizenzen aufgebraucht sind.
Systemnachricht	
Keine weiteren Einstellungen verfügbar.	
Ausstehende Requests	
x Tage seit Request-Erstellung	Legt die Anzahl an Tagen fest, welche seit der Request-Erstellung vergangen sein müssen, bevor für diesen Request eine Benachrichtigung erstellt wird, sollte dieser noch ungenehmigt sein.
Anwenden auf	Legt fest, ob die Benachrichtigung für alle Requests oder für Requests nach bestimmten Filterkriterien erstellt werden soll. Sie können mehrere Filter hinzufügen. Jeder Filter prüft dabei auf Quelle, Modus, Typ oder Status. Ein * im Feld bedeutet "Alle". Die einzelnen Felder eines Filters sind UND-verknüpft (=alle Einstellungen müssen auf den Request zutreffen), die einzelnen Filter sind ODER-verknüpft (=zumindest einer der ausgewählten Filter muss zutreffen).
Priorität	Legt fest, mit welcher Priorität die Benachrichtigungen für diese Requests angelegt werden. Hinweis: Diese Benachrichtigung kann mehrfach angelegt werden. Wenn Sie für unterschiedliche Requests unterschiedliche Prioritäten benötigen, dann legen Sie diese Benachrichtigung einfach öfter mit unterschiedlichen Filtern an.
Keine Benachrichtigung wenn keine ausstehenden Requests	Ist diese Einstellung aktiviert, wird keine Benachrichtigung versendet, wenn es keine ausstehenden Requests nach den ausgewählten Kriterien gibt. Ist diese Einstellung nicht aktiviert (Standard), erhalten Sie auch dann eine E-Mail, wenn es keine Requests gibt. Sie werden dann über den Umstand benachrichtigt, dass es keine ausstehenden Requests gibt.

Die Übersicht über die Einstellungsmöglichkeiten der von Plugins bereitgestellten Benachrichtigungen finden Sie in den Kapiteln des jeweiligen Plugins.

12.4.3 Übersicht

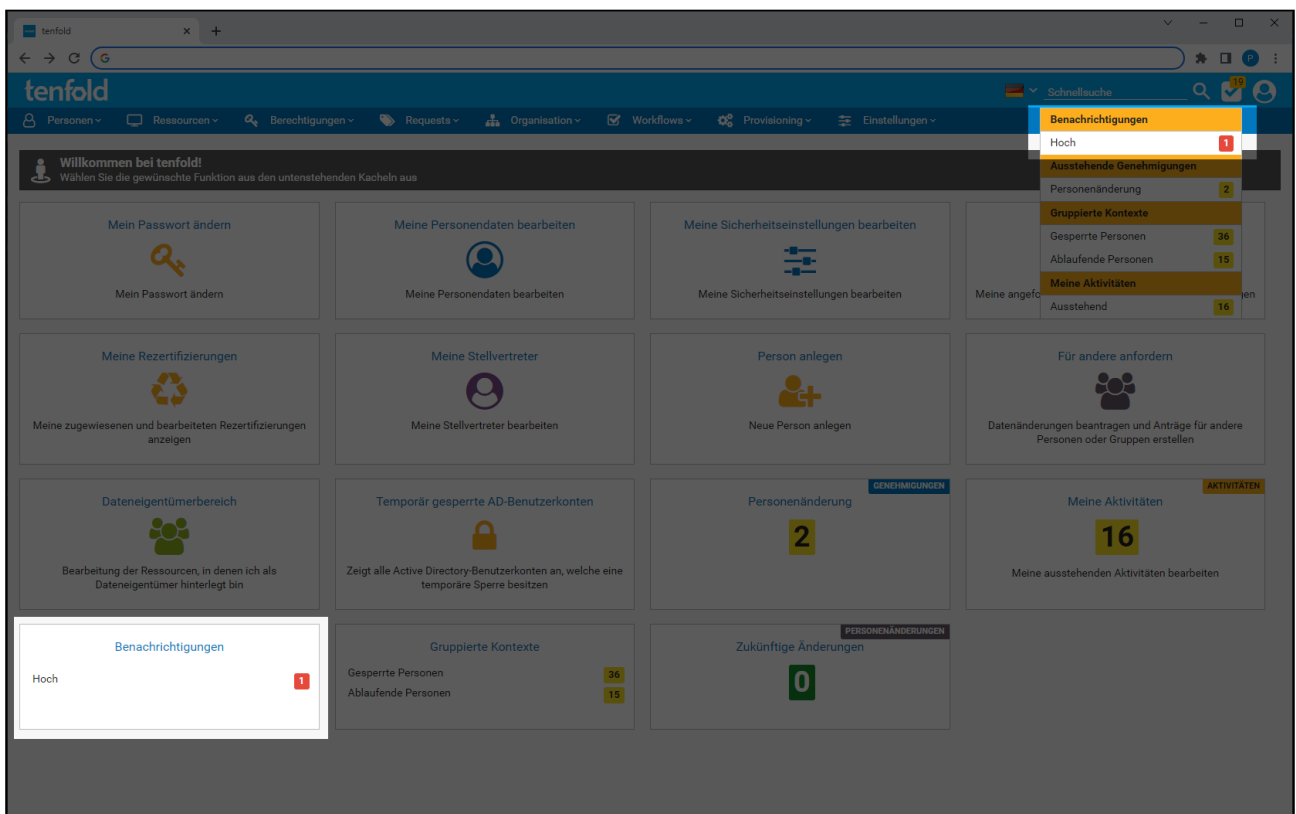
Nachdem Benachrichtigungen erstellt wurden, können diese in tenfold eingesehen und bearbeitet werden.

Sie können die Übersicht über die Benachrichtigungen auf mehrere Arten aufrufen. Für eine Übersicht aller Benachrichtigungen, navigieren Sie im Menü zu *Einstellungen > Benachrichtigungen > Übersicht*.

Benötigte Berechtigung

Für die Anzeige aller Benachrichtigungen wird die Berechtigung "View Alerts" (9204) benötigt.

Möchten Sie nur jene Benachrichtigungen anzeigen, für die Sie zuständig sind, verwenden Sie die Links für die jeweilige Benachrichtigungspriorität in der Kachel "Benachrichtigungen" auf der Startmaske von tenfold, oder im Nachrichten-Dropdown neben der Schnellsuche.



Benötigte Berechtigung

Eine spezielle Berechtigung zur Anzeige der eigenen Benachrichtigungen ist nicht erforderlich.

Anzeige

Sowohl die Kachel als auch der Eintrag im Dropdown-Menü werden nur angezeigt, wenn Benachrichtigungen für Sie vorhanden sind, die nicht abgeschlossen sind.

Auf der Maske angelangt können Sie die Anzeige anhand der folgenden Felder filtern:

- Status der Berechtigung
- Typ der Berechtigung
- Beschreibung
- Zeitraum, in dem die Benachrichtigung angelegt wurde (Start- und Enddatum)

Im Aktionsmenü können Sie mit der Aktion "Anzeigen" weitere Details zur Benachrichtigung einblenden.

The screenshot shows the tenfold web interface. At the top, there's a navigation bar with tabs like 'Personen', 'Ressourcen', 'Berechtigungen', 'Requests', 'Organisation', 'Workflows', 'Provisioning', and 'Einstellungen'. Below this, a notification banner states 'Job 'Alert Pending Requests - Sync' ist fehlgeschlagen' with buttons 'Bestätigen' and 'Abbrechen'. The main content area has two tabs: 'Benachrichtigung' (selected) and 'Kanäle'. Under 'Benachrichtigung', there are sections for 'Allgemein' (General) and 'Details'. The 'Allgemein' section shows 'Erstellt am' (Created at) as 16.09.2022 00:00:00, 'Priorität' (Priority) as HOCH, and 'Status' as OFFEN. The 'Details' section shows 'Name' as Alert Pending Requests - Sync, 'Startdatum' (Start date) as 16.09.2022 00:00:00, 'Enddatum' (End date) as 16.09.2022 00:00:00, 'Laufzeit' (Runtime) as 00:00:00, and 'Status' as FEHLGESCHLAGEN. Below these is a 'Fehlermeldung' (Error message) section containing a stack trace starting with 'at.certex.ism.exception.jobs.JobExecutionException: org.codehaus.groovy.control.MultipleCompilationErrorsException: startup failed:'. The stack trace includes details about a failed import in a Groovy script and a subsequent error in the job execution control.

Im Karteireiter "Benachrichtigung" finden Sie Details, die, neben allgemeinen Informationen wie Status, Priorität oder Erstellungszeitpunkt, spezifisch die jeweilige Benachrichtigung betreffen.

Im Karteireiter "Kanäle" finden Sie eine Auflistung aller Kanäle, über welche die Benachrichtigung versendet wurde und ob der Versand erfolgreich war.

Außerdem haben Sie mit der Aktion "Bestätigen" die Möglichkeit, die Benachrichtigung abzuschließen, damit andere für diese Benachrichtigung verantwortlichen Personen darüber informiert werden, dass diese Benachrichtigung kein weiteres Eingreifen mehr benötigt.

Sollte die Benachrichtigung im Status "Fehlgeschlagen" sein, so können Sie mit der Aktion "Erneut senden" einen erneuten Versandversuch starten.

Mit der Schaltfläche "Mehrfachänderung starten" können Sie mehrere Benachrichtigungen auswählen, um daraufhin die gewählte Aktion für alle ausgewählten Benachrichtigungen durchzuführen. Mit der Schaltfläche "Mehrfachänderung beenden" wird keine Änderung durchgeführt. Mit der Schaltfläche "Aktion für Auswahl" wählen Sie eine Aktion aus, welche anschließend für alle gewählten Benachrichtigungen durchgeführt wird.

Aktion auswählen

Sie können nur Aktionen wählen, welche auf alle ausgewählten Benachrichtigungen anwendbar ist.

12.5 Berechtigungen

12.5.1 Berechtigungen

Alle Funktionen von tenfold sind über Berechtigungen vor unerlaubter Verwendung geschützt. tenfold unterscheidet zwei Arten von Berechtigungen: Vordefinierte Berechtigungen und benutzerdefinierte Berechtigungen.

Vordefinierte Berechtigungen sind bereits bei der Installation von tenfold im System vorhanden und können nicht gelöscht werden. Sie erlauben die Nutzung bestimmter Funktionen in tenfold, wie beispielsweise die Änderung bestimmter Stammdaten oder Einstellungen.

Benutzerdefinierte Berechtigungen werden vom Administrator verwaltet. Sie haben für tenfold zu Beginn keine Bedeutung, können aber für bestimmte Bereiche und Aktionen hinterlegt werden, sodass Anwender, welche die jeweilige Funktion nutzen wollen, über die entsprechende hinterlegte Berechtigung verfügen müssen. Beispielsweise lassen sich bei Genehmigungsworkflows für die einzelnen Schritte Berechtigungen festlegen, die ein Benutzer benötigt, um einen Request in diesem Schritt genehmigen zu können.

12.5.2 Rollen

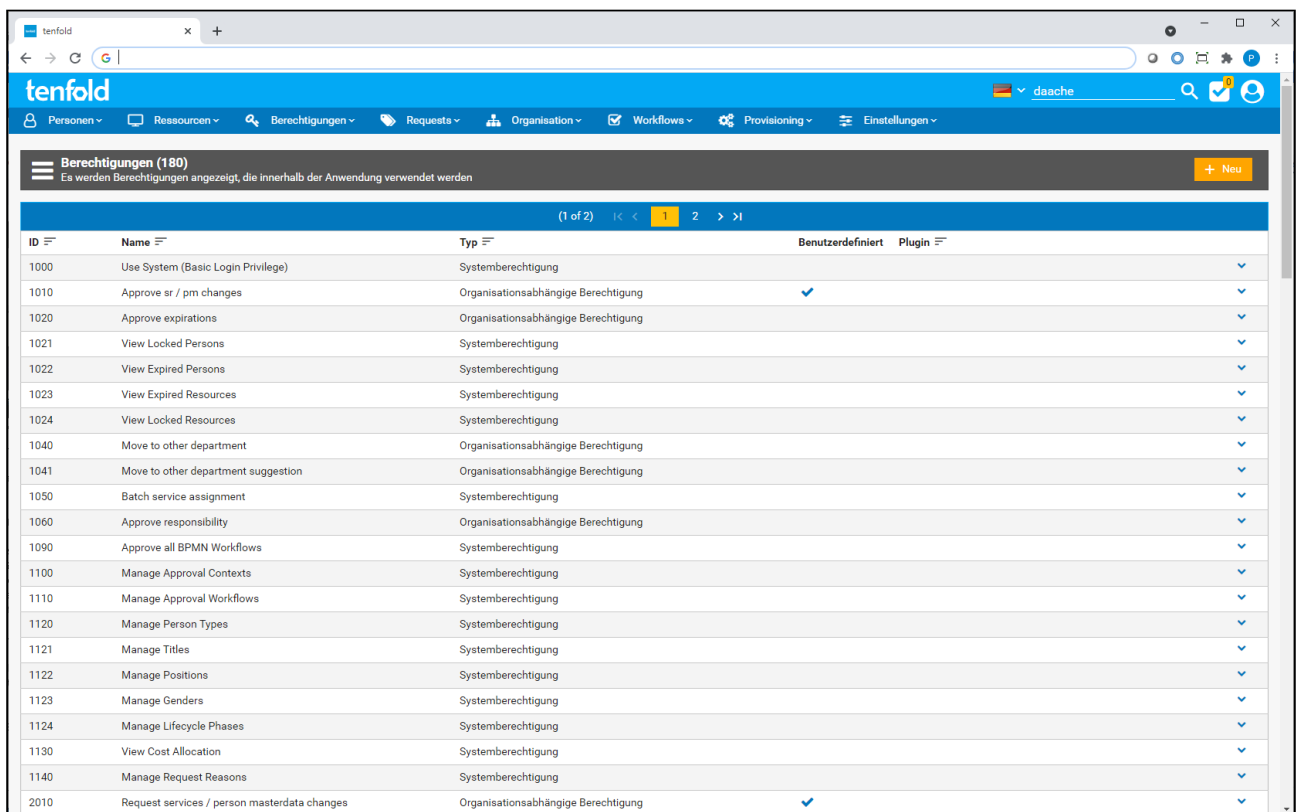
Rollen sind eine Zusammenfassung von Berechtigungen, die Benutzern zugeordnet werden können. In tenfold werden Berechtigungen ausschließlich über Rollen zugeordnet und können einem Benutzer nicht direkt zugewiesen werden. Ein Benutzer kann mehrere Rollen besitzen und jede Rolle kann ihm für bestimmte Organisationseinheiten oder für alle Organisationseinheiten zugeordnet werden. Ein Benutzer erhält hierbei die Summe aller Berechtigungen für alle Organisationseinheiten, für die ihm Rollen zugeordnet wurden. Vordefinierte Berechtigungen haben hierbei einen Gültigkeitsbereich (siehe Abschnitt "Vordefinierte Berechtigungen"). Berechtigungen mit dem Gültigkeitsbereich "System" haben keinen Bezug zu Organisationseinheiten und gelten global.

12.5.3 Verwaltung der Berechtigungen

Zur Anzeige der vordefinierten Berechtigung, sowie zur Verwaltung von benutzerdefinierten Berechtigungen, gelangt man über den Menüpunkt *Einstellungen > tenfold Berechtigungen > Berechtigungen*.

Benötigte Berechtigung

Um diese Funktion nutzen zu können, ist die Systemberechtigung "Manage Privileges (tenfold)" (7030) erforderlich.



ID	Name	Typ	Benutzerdefiniert	Plugin
1000	Use System (Basic Login Privilege)	Systemberechtigung		
1010	Approve sr / pm changes	Organisationsabhängige Berechtigung	✓	
1020	Approve expirations	Organisationsabhängige Berechtigung		
1021	View Locked Persons	Systemberechtigung		
1022	View Expired Persons	Systemberechtigung		
1023	View Expired Resources	Systemberechtigung		
1024	View Locked Resources	Systemberechtigung		
1040	Move to other department	Organisationsabhängige Berechtigung		
1041	Move to other department suggestion	Organisationsabhängige Berechtigung		
1050	Batch service assignment	Systemberechtigung		
1060	Approve responsibility	Organisationsabhängige Berechtigung		
1090	Approve all BPMN Workflows	Systemberechtigung		
1100	Manage Approval Contexts	Systemberechtigung		
1110	Manage Approval Workflows	Systemberechtigung		
1120	Manage Person Types	Systemberechtigung		
1121	Manage Titles	Systemberechtigung		
1122	Manage Positions	Systemberechtigung		
1123	Manage Genders	Systemberechtigung		
1124	Manage Lifecycle Phases	Systemberechtigung		
1130	View Cost Allocation	Systemberechtigung		
1140	Manage Request Reasons	Systemberechtigung		
2010	Request services / person masterdata changes	Organisationsabhängige Berechtigung	✓	

Folgende Tätigkeiten können ausgeführt werden:

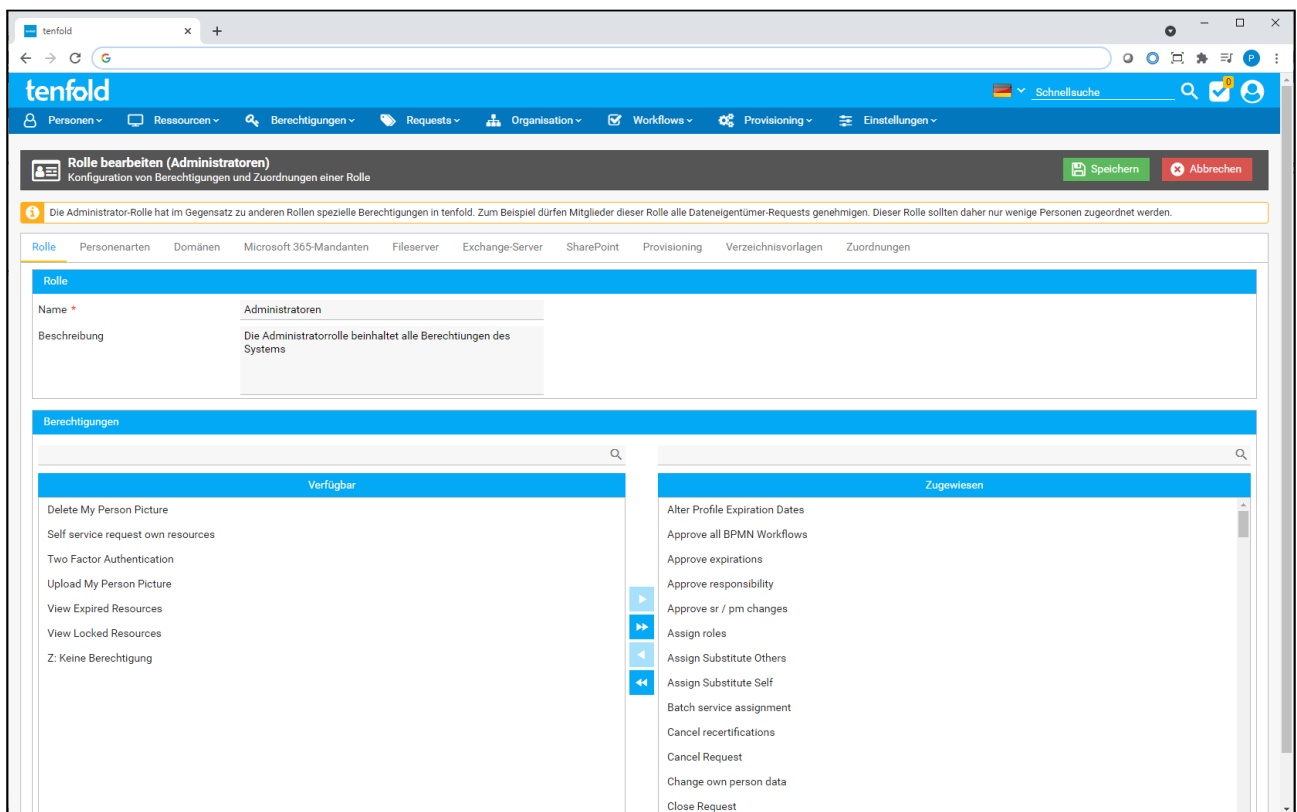
- Anlegen einer neuen, benutzerdefinierten Berechtigung über den Button "Neu"
- Bearbeiten von bestehenden Berechtigungen
- Löschen von benutzerdefinierten Berechtigungen (sofern diese nicht bereits verwendet werden)

Warnung

Ändern Sie keinesfalls Einstellungen (Name oder Gültigkeitsbereich) von vordefinierten Berechtigungen.

12.5.4 Rollen

Zur Verwaltung der Rollen gelangt man über den Menüpunkt *Einstellungen* > *tenfold Berechtigungen* > *Rollen*.



Um eine neue Rolle anzulegen oder eine bestehende Rolle zu bearbeiten, gehen Sie wie folgt vor:

- Auf der Liste aller Rollen klicken Sie auf den Button "Neu", bzw. wählen Sie "Bearbeiten" aus dem Kontextmenü der betroffenen Rolle
- Vergeben Sie einen sprechenden Namen und fügen Sie gegebenenfalls einen beschreibenden Text hinzu

Die Erklärung der Inhalte, aus denen eine Rolle besteht, erfolgt in den nachfolgenden Abschnitten, wobei jeder Abschnitt sich auf einen der Karteireiter bezieht.

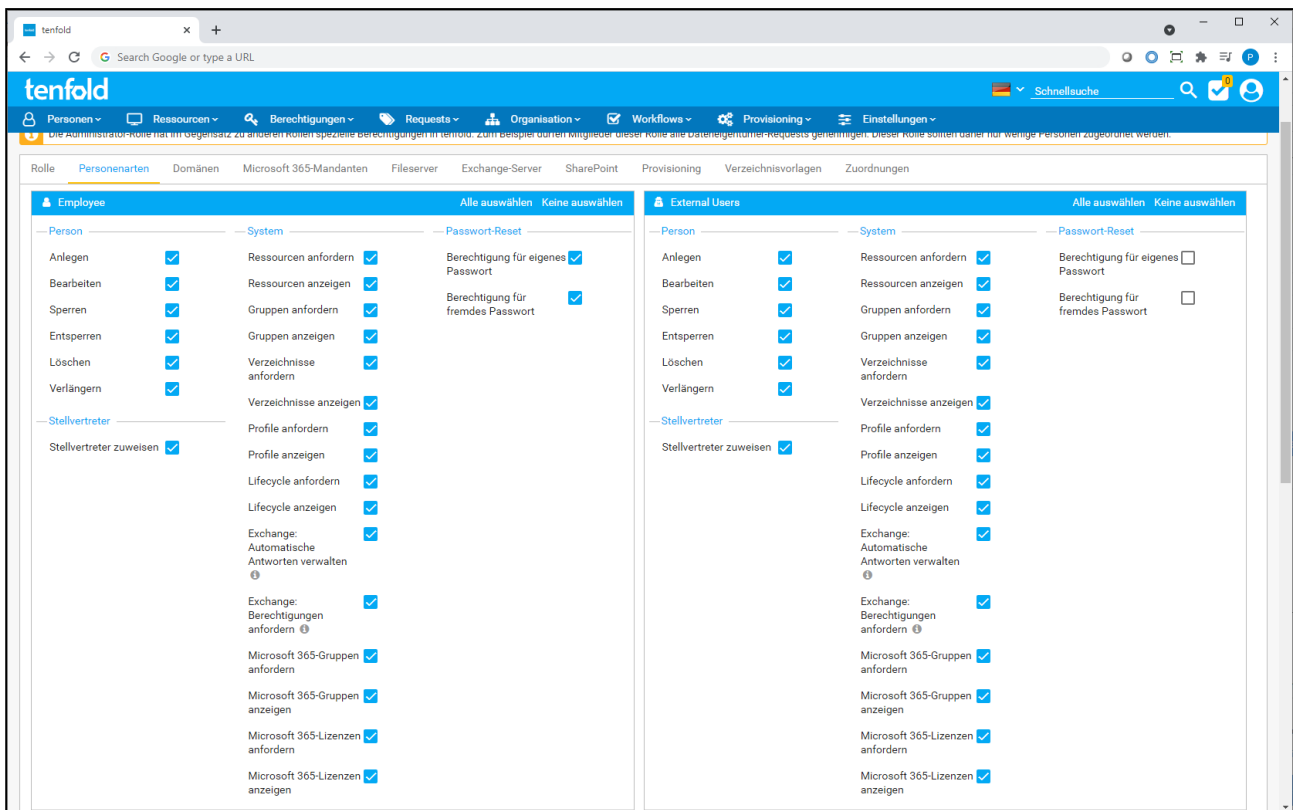
Einzelberechtigungen / Karteireiter "Rolle"

Auf dem Karteireiter "Rolle" können die Einzelberechtigungen der Rolle zugeordnet werden. Nicht der Rolle zugewiesene Berechtigungen erscheinen auf der linken Seite im Bereich "Verfügbar" und Berechtigungen, die der Rolle zugewiesen sind, erscheinen im Bereich "Zugewiesen".

Tipp

Über die beiden Eingabefelder über den Bereichen "Verfügbar" und "Zugewiesen" können Berechtigungen nach einem Suchbegriff gefiltert werden.

Personenarten



In diesem Abschnitt wird festgelegt, welche Aktionen mit der Rolle für die unterschiedlichen Personenarten erlaubt sind. Jede Personenart wird durch einen eigenen Bereich abgebildet, in dem die jeweiligen Aktionen aktiviert oder deaktiviert werden können.

Einschränkungen

Beachten Sie, dass sich die ausgewählten Funktionen immer auf die entsprechende Personenart beziehen. Der Bezug kann jedoch weiter eingeschränkt werden, wenn die Rolle einer Person nur für eine bestimmte Organisationseinheit zugeordnet wurde. Wird, beispielsweise, in der Rolle für eine Personenart die Aktion "Ressourcen anfordern" aktiviert und die Rolle dann einer Person mit Einschränkung auf eine bestimmte Abteilung zugeordnet, so kann diese Person Ressourcen nur für Personen der in der Rolle definierten Art und der in der Zuordnung definierten Abteilung anfordern.

Domänen

Im Abschnitt "Domänen" können die Berechtigungen festgelegt werden, welche für diese Rolle in den unterschiedlichen Domänen gelten. Jede konfigurierte Active Directory-Domain wird in einer Zeile abgebildet. Existiert nur eine Domain, so wird nur eine Zeile angezeigt. In den Spalten können bestimmte Funktionen, die sich allesamt auf Objekte der jeweiligen Domain beziehen, aktiviert werden.

Es gilt dabei zu beachten, dass es sich hierbei, so wie bei allen vergleichbaren Berechtigungen zum "Bearbeiten", "Löschen", usw., immer nur um die Berechtigung handelt, mit der man eine solche Aktion anfordern kann (einen Request erstellen). Ob die Änderung dann tatsächlich durchgeführt wird, hängt von der Konfiguration der Genehmigungsworkflows ab. Nachfolgende Aktionen stehen zur Auswahl:

Bezeichnung	Beschreibung
Anlegen von Gruppen	Erlaubt das Anlegen von neuen Active Directory-Gruppen in dieser Domain.
Anzeigen	Erlaubt das Anzeigen von Benutzer- und Gruppenobjekten in dieser Domain.
Bearbeiten	Erlaubt das Bearbeiten von Gruppennamen und Beschreibungen in dieser Domain.
Löschen	Erlaubt das Löschen von Gruppen in dieser Domain.
Gruppenmitglieder bearbeiten	Erlaubt das Hinzufügen oder Löschen von Mitgliedern zu Gruppen in dieser Domain.
Gruppen-Dateneigentümer bearbeiten	Erlaubt das Bearbeiten der Dateneigentümer für Gruppen in dieser Domain.

Wurde im Bereich "Einschränkungen" im Feld "Auswahl" die Option "Keine Einschränkungen" gewählt, so gelten die oben getroffenen Einstellungen für alle Gruppen in den jeweiligen Domains. Durch eine Änderung auf die Einstellung "Einschränken auf Organisationseinheiten" können Sie die vergebenen Berechtigungen auf bestimmte Organisationseinheiten in Ihrem Active Directory einschränken.

Wählen Sie im Abschnitt "Erlaubte Organisationseinheiten" jene Organisationseinheiten aus, in denen diese Personen Gruppen bearbeiten dürfen. Dies schließt auch untergeordnete Organisationseinheiten ein. Sie können im Abschnitt "Ausgeschlossene Organisationseinheiten" Organisationseinheiten auswählen, deren Bearbeitung durch diese Rolle ausgeschlossen werden soll.

Sollten für eine Domäne keine erlaubten Organisationseinheiten definiert werden, können in der Domäne weiterhin alle Gruppen bearbeitet werden, es sei denn, sie befinden sich in ausgeschlossenen Organisationseinheiten. Sollten sich erlaubte und ausgeschlossene Organisationseinheiten überschneiden, haben ausgeschlossene Organisationseinheiten Vorrang. Dies bedeutet, dass Gruppen darin dann nicht verwaltet werden können.

Stellvertreter

Da Stellvertreter (siehe [Stellvertretungen](#)(see page 372)) die Gesamtmenge der eigenen und der stellvertretenden Person erhalten, bedeutet dies, dass auch hier ausgeschlossene Organisationseinheiten Vorrang haben.

Beispiel: Person A wird von Person B stellvertreten. Person A darf alle Gruppen der Domäne bearbeiten. Person B (Stellvertreter) ist Mitglied einer Rolle, in welcher die Organisationseinheit "IT" explizit ausgeschlossen wurde. Trotz der Stellvertretung darf Person B Gruppen in dieser Organisationseinheit nicht bearbeiten.

Microsoft 365-Mandanten

Hier können Sie zu jedem eingerichteten Microsoft 365-Mandanten Berechtigungen vergeben, die notwendig sind, um verschiedene Aktionen auf diesen Mandanten mit tenfold durchzuführen.

Berechtigung	Beschreibung
Gruppen anzeigen	Erlaubt es einer Person mit dieser Rolle, die Gruppen auf der Maske "Microsoft 365-Gruppen" (siehe Verwaltung der Microsoft 365 Gruppen (see page 331)) anzuzeigen und deren Mitglieder auszulesen.
Gruppenmitglieder bearbeiten	Erlaubt es, die Mitglieder von Gruppen auf diesem Mandanten zu bearbeiten.
Gruppen-Dateneigentümer bearbeiten	Erlaubt es, die Dateneigentümer der Gruppen zu bearbeiten.
Gruppen-Besitzer bearbeiten	Erlaubt es, die Besitzer der Gruppen zu bearbeiten.
Lizenzen anzeigen	Erlaubt es, die Lizenzen dieses Mandanten anzuzeigen (siehe Verwaltung der Microsoft 365 Lizenzen (see page 324)).
Lizenzen bearbeiten	Erlaubt es, in tenfold die Zuordnungen der Lizenzen zu Anwendern zu verwalten.
Lizenzen-Dateneigentümer bearbeiten	Erlaubt es, die Dateneigentümer der Lizenzen zu verwalten.
Teams anzeigen	Erlaubt es, die Teams des Mandanten in tenfold anzuzeigen (siehe Microsoft Teams (see page 337)).
Geteilte OneDrive-Inhalte anzeigen	Erlaubt die Anzeige der OneDrive-Inhalte auf der Maske "Geteilte Microsoft 365-Inhalte" (siehe Geteilte Microsoft 365-Inhalte).
Geteilte Microsoft SharePoint-Inhalte anzeigen	Erlaubt die Anzeige der geteilten SharePoint-Inhalte dieses Mandanten.
Geteilte Microsoft Teams-Inhalte anzeigen	Erlaubt die Anzeige der geteilten Teams-Inhalte dieses Mandanten.

Fileserver

Der Abschnitt "Fileserver" erlaubt es, individuelle Berechtigungen auf einzelne Fileserver zu setzen. Analog zu den Domains ist jeder Fileserver als Zeile dargestellt. Nachfolgende Aktionen stehen für Fileserver zur Auswahl:

Bezeichnung	Beschreibung
Anzeigen	Erlaubt es, den Fileserver mit allen Verzeichnissen und Berechtigungen in der Administrationsmaske anzuzeigen
Bearbeiten	Erlaubt die Bearbeitung des Fileservers in der Administrationsmaske

Exchange-Server

Im Abschnitt "Exchange-Server" können, für jeden konfigurierten Exchange-Server, individuell Berechtigungen vergeben werden. Jeder Server erhält dabei einen eigenen Bereich. Bei Exchange-Servern wird nicht zwischen Anzeige und Bearbeitung unterschieden, sondern es können, je nach Kategorie (Benutzerpostfach, Öffentliche Postfächer), die Berechtigungen, auf Ebene des Postfachs selbst und auf Ebene des Postfachordners, zur Anzeige und Bearbeitung festgelegt werden.

SharePoint

Für SharePoint ist es im Abschnitt "SharePoint" möglich, für jeden konfigurierten Server zu steuern, ob die Objekte und Berechtigungen des jeweiligen SharePoint-Servers angezeigt werden können.

Provisioning

In diesem Karteireiter können Sie bestimmen, welche manuellen Aktivitäten ein Mitglied dieser Rolle abschließen kann. In der Tabelle wird, für jeden manuellen Provisionierungsschritt jeder Ressource, eine Zeile angezeigt.

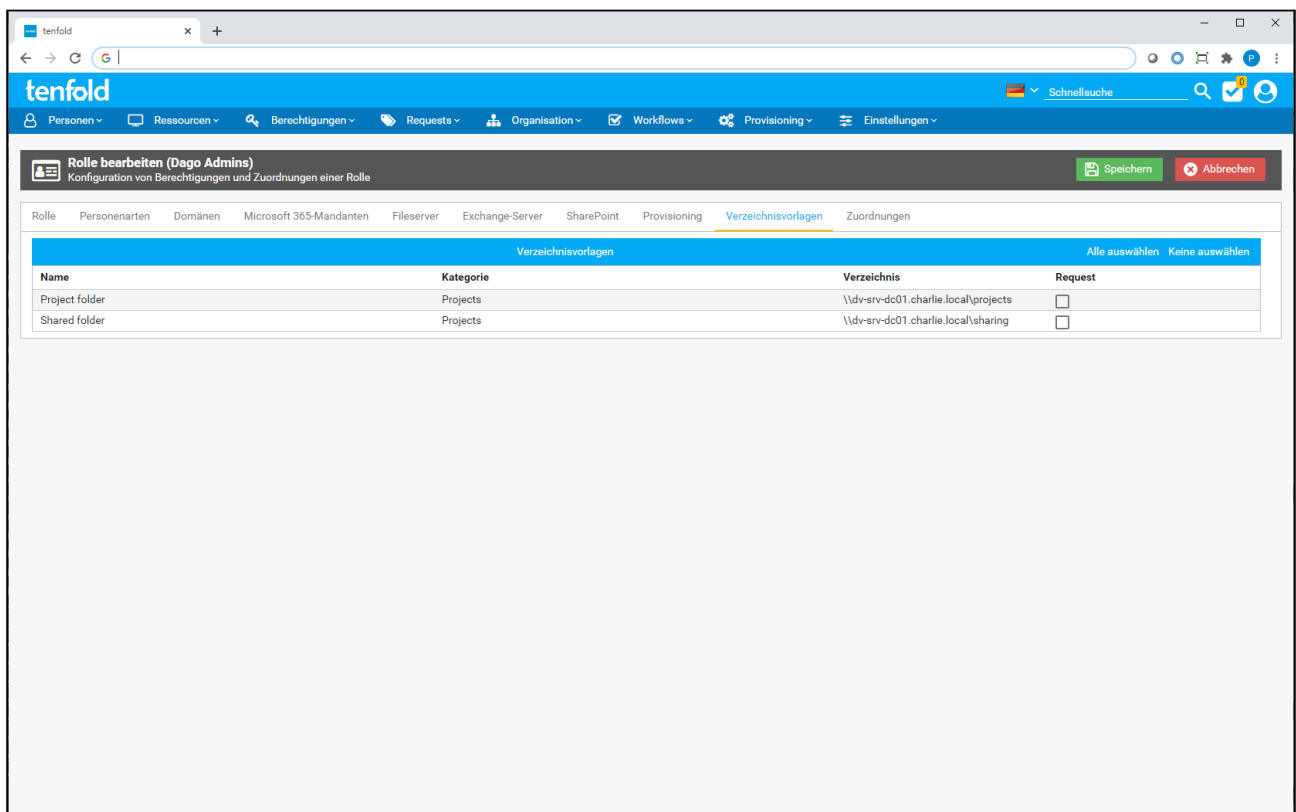
The screenshot shows the 'tenfold' web interface. The top navigation bar includes 'Personen', 'Ressourcen', 'Berechtigungen', 'Requests', 'Organisation', 'Workflows', 'Provisioning', and 'Einstellungen'. The 'Provisioning' tab is active, showing a list of provisioning steps on the left. The 'Send mail (E-Mail-Benachrichtigung)' step is selected, and its configuration is shown on the right. The configuration includes a table with the following settings:

Benachrichtigungsart	Betreff überschreiben	Absender	Absender-Adresse	Empfänger festlegen	Verhalten bei Neuanlage *	E-Mail ausschließlich für Ressourcenrequest
Standard Provisionierungsnachricht versenden	<input type="checkbox"/>	Systemeinstellung übernehmen	support@certex.at	Personen, die für Schließen oder Abbrechen berechtigt sind	Angeforderte Berechtigungen einfügen	<input checked="" type="checkbox"/>
					Requestbemerkung einfügen	<input type="checkbox"/>
					Request Ticketnummer einfügen	<input type="checkbox"/>
					Ressourcenbeschreibung einfügen	<input type="checkbox"/>
					Lösungsbeschreibung d. Ressource einfügen	<input type="checkbox"/>
					Schließen Link einfügen	<input checked="" type="checkbox"/>
					Abbrechen Link einfügen	<input checked="" type="checkbox"/>
					Berechtigungsmodus *	Berechtigungsvergabe über tenfold-Rollen
					Blockierende Aktivität erstellen	<input checked="" type="checkbox"/>

Zum Beispiel fügt das E-Mail Benachrichtigungs-Plugin für jeden Provisionierungsschritt, welcher über einen Schließen-Link verfügt und bei der die Einstellung "Berechtigungsvergabe über tenfold-Rollen" ausgewählt wurde, eine Zeile in dieser Tabelle an. Genauere Informationen finden Sie bei der Beschreibung der jeweiligen Plugins.

Verzeichnisvorlagen

Hier können Sie, zu jeder erstellten Verzeichnisvorlage, festlegen, ob Mitglieder dieser Rolle Verzeichnisse nach der gewählten Vorlage bestellen dürfen.

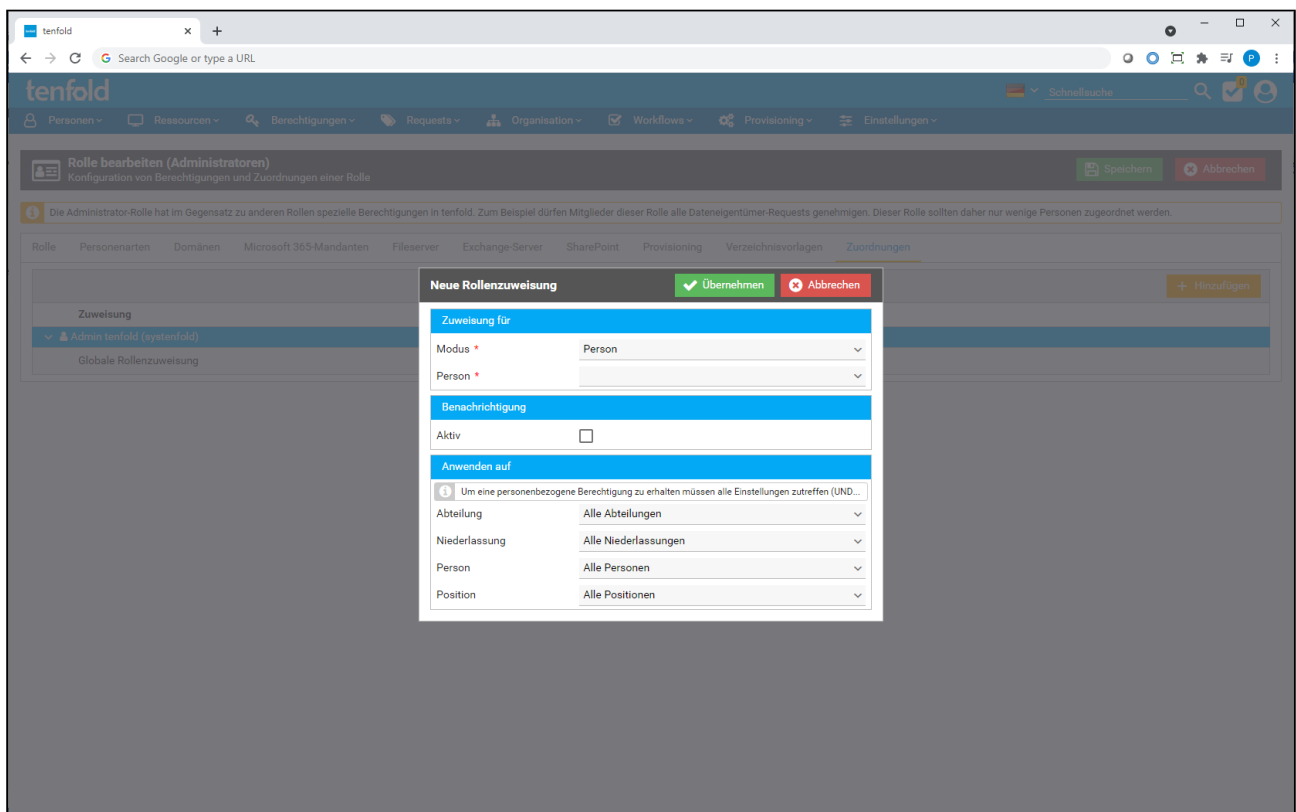


12.5.5 Rollenzuordnung

Damit ein Benutzer die Berechtigungen erhält, die in der Rolle definiert sind, muss die Rolle dem Benutzer zugeordnet werden. Gehen Sie folgendermaßen vor, um einem Benutzer eine Rolle zuzuordnen:

Die Zuordnung erfolgt immer von der Rolle aus. Navigieren Sie daher im Menü auf *Einstellungen > tenfold Berechtigungen > Rollen*.

1. Wählen Sie "Bearbeiten" im Kontextmenü der jeweiligen Rolle
2. Wechseln Sie auf den Karteireiter "Zuordnungen"
3. Klicken Sie auf Hinzufügen - es öffnet sich ein Dialog



1. In dem Dialog wählen Sie nun die Person oder AD-Gruppe aus, welcher die Rolle zugeordnet werden soll.
2. Darüber hinaus wählen Sie die Organisationseinheiten aus, auf welche die Rolle beschränkt werden soll.
3. Klicken Sie anschließend auf den Button "Übernehmen", um den neuen Eintrag zu sichern
4. Abschließend muss die Rolle selbst gesichert werden. Dies erfolgt durch Klick auf den Button "Speichern".

Um Ihre Einstellungen zu testen, können Sie anschließend eine Anmeldung mit dem jeweiligen Benutzer durchführen. Nutzen Sie dafür die Funktion "Session ändern" - siehe [Sessionverwaltung](#) (see page 521).

Eigene Organisationseinheiten

Zusätzlich können, über die Kontrollkästchen, Berechtigungen für die eigene Abteilung, die eigene Niederlassung sowie den eigenen Vorgesetzten gesetzt werden. Damit wird verhindert, dass, bei einem Organisationswechsel (die Person wechselt z.B. in eine andere Abteilung), die Änderungen an der Rollenzuordnung manuell nachgezogen werden muss.

Zuordnungen können auf folgende Organisationsstrukturen eingeschränkt werden:

Anwenden auf	Beschreibung
Abteilung	Die Rolle wird auf alle Personen angewendet, welche sich innerhalb der ausgewählten Abteilung befinden.

Anwenden auf	Beschreibung
Unternehmen	Die Rolle wird auf alle Personen angewendet, welche sich in einer Niederlassung befinden, welche zum ausgewählten Unternehmen gehört.
Niederlassung	Die Rolle wird auf alle Personen angewendet, welche sich in der ausgewählten Niederlassung befinden.
Person	Die Rolle wird auf die ausgewählte Person angewendet. Die Auswahl "Personen anhand von Vorgesetztem" bedeutet, dass sich die Rolle auf alle Personen bezieht, welche den angemeldeten Benutzer als Vorgesetzten eingetragen haben. Achtung: Dies bezieht sich nur auf direkt vorgesetzte Personen. Vorgesetzte von Vorgesetzten werden nicht unterstützt.
Position	Die Rolle wird auf alle Personen angewendet, welche die ausgewählte Position zugeordnet haben. Hinweis: Dies bezieht sich auf das Auswahlfeld "Position" (POSITION) und nicht auf das Freitextfeld "Stellenbezeichnung" (JOB_TITLE).

Mehrere Einschränkungen und Zuordnungen

Sollten bei einer Zuordnung mehrere Einschränkungen getroffen werden (z.B. eine Einschränkung auf Niederlassung und Abteilung) so gilt die Zuordnung nur für Personen, auf welche **alle** gewählten Einschränkungen zutreffen (Und-Verknüpfung). Sollte einer Person eine Rolle mehrfach zugeordnet werden, so gilt die Gesamtmenge alle zutreffenden Personen (Oder-Verknüpfung).

12.5.6 Auswertung

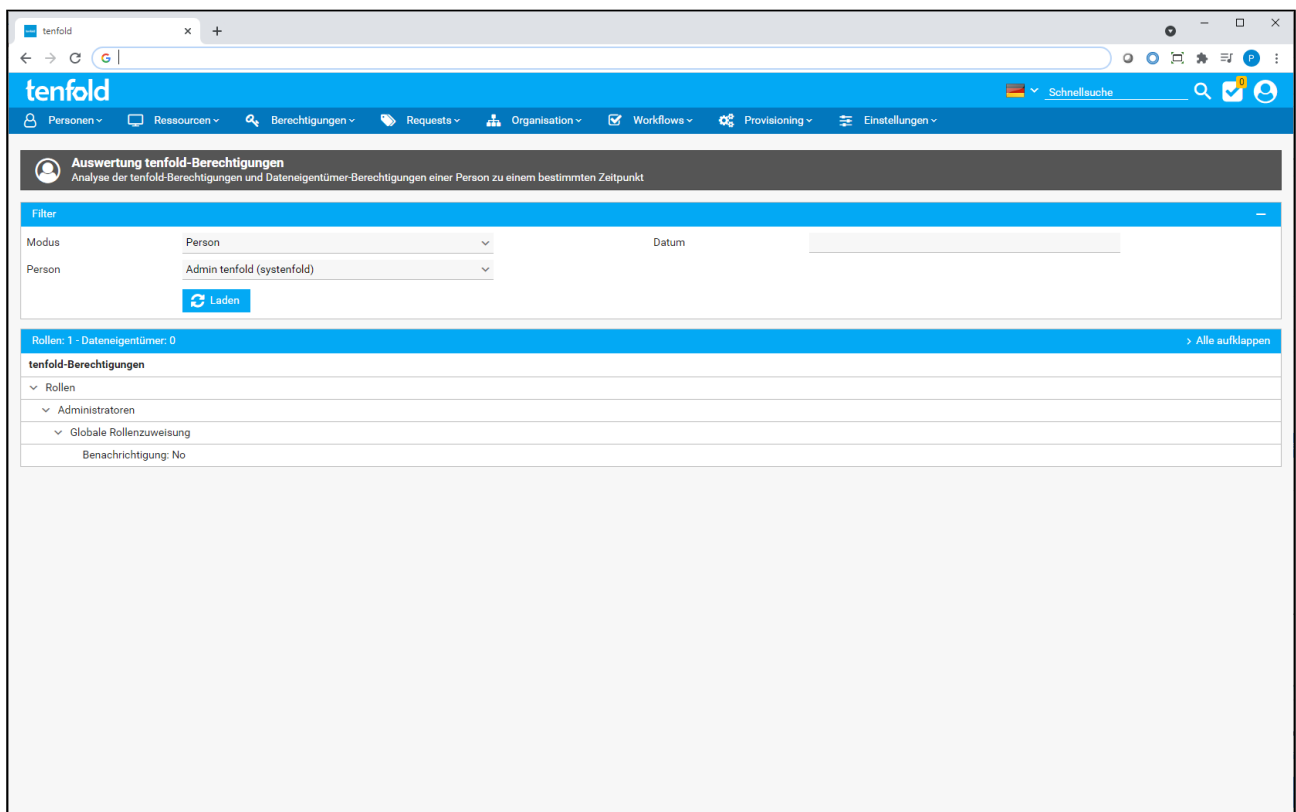
Mit der Berechtigungsauswertung kann man die Zuordnungen der unterschiedlichen tenfold-Berechtigungen übersichtlich darstellen. Die Auswertung ist über das Menü *Einstellungen > tenfold-Berechtigungen > Auswertung* erreichbar.

Benötigte Berechtigung

Für die Verwendung der Auswertung ist die Systemberechtigung "Role Definition" (7020) erforderlich.

Die Maske unterstützt zwei unterschiedliche Modi:

- Person: Es werden alle Berechtigungen (inklusive Dateneigentümerberechtigungen) für die ausgewählte Person zum ausgewählten Zeitpunkt dargestellt.
- Berechtigung: Es wird angezeigt, wo die ausgewählte Berechtigung verwendet wird. Es werden in der Baumansicht dabei zwei Knoten angezeigt: einer zeigt, welchen Rollen die Berechtigung zugeordnet ist (mit Unterknoten, die zeigen, welchen Personen diese Rolle zugeordnet wurde) und einer zeigt, welche Personen diese Berechtigung zugeordnet haben (und über welche Rolle dies geschieht).



12.5.7 Vordefinierte Berechtigungen

Folgende Berechtigungen sind in tenfold bereits vordefiniert:

ID	Name	Beschreibung (Erlaubt die angegebene Aktion)	Gültigkeitsbereich
8551	Align Generated Values	Erlaubt den Abgleich von generierten Werten.	System
2091	Align Person Links	Erlaubt den Abgleich von Personendaten über verknüpfte Personen.	
3090	Alter Profile Expiration Dates	Erlaubt es, den Profilen einer Person ein Ablaufdatum zuzuordnen.	System
1020	Approve Expirations	Ablaufende Personen können verlängert werden.	Organisation
1090	Approve Person-based BPMN Workflows	Alle personenbezogenen Genehmigungsschritte (Vorgesetzter, Skript, etc.) in BPMN-Genehmigungsworkflows können genehmigt werden.	System
1060	Approve Responsibility	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	

1010	Approve sr / pm changes	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	
7010	Assign roles	Einer Person Rollen zuzuweisen.	Organisation
7051	Assign Substitute Others	Für eine andere Person Stellvertreter festlegen.	Organisation
7050	Assign Substitute Self	Für sich selbst Stellvertreter festlegen.	System
1050	Batch service assignment	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	
8312	Cancel Recertifications	Offene Rezertifizierungsprozesse können abgebrochen werden.	System
3050	Cancel Requests	Requests können abgebrochen werden.	Organisation
2020	Change Own Person Data	Bearbeitung der eigenen Stammdaten.	System
9230	Change Scheduled Request Execution Time	Erlaubt es, das Durchführungsdatum von geplanten Requests zu ändern.	System
3040	Close Request	Ein Request kann abgeschlossen werden.	Organisation
8010	Configuration Administration	Die Systemparameter können geändert werden.	System
8221	Create Active Directory Groups	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	
2200	Data Correction External Systems	Die Funktion <i>Datenkorrektur</i> kann verwendet werden.	System
8115	Delete My Person Picture	Das Bild der eigenen Person kann entfernt werden.	System
8113	Delete Person Picture	Bilder von Personen können entfernt werden.	System
1200	Default Data Owner Active Directory	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	
8020	Department Administration	Verwaltung der Abteilungen.	System

2070	Edit Person Expert Mode	Anzeige des Tabs "Ressourcen" auf der Maske "Person bearbeiten" im Bearbeiten-Modus.	System
3061	Edit Profile Assignments	Profilzuordnungen können bearbeitet werden.	System
8330	EX Resource Group Configuration Administration	Die Einstellungen zu den Exchange-Berechtigungsgruppen können verwaltet werden.	System
8331	Ex Rights administration	Erlaubt die Verwaltung der Exchange-Berechtigungsstufen (z.B. Konfigurieren der Suffixe für Berechtigungsgruppen, Verfügbarkeit im Self-Service).	System
3103	Export Active Directory Report	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	
3105	Export Exchange Report	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	
3101	Export FS Report	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	
9221	Export Microsoft 365 Report	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	
3109	Export Service Assignment Report	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	
3107	Export SharePoint Report	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	
8330	EX Ressource Group Configuration	Bearbeitung der Exchange-Gruppenkonfiguration.	System
8331	EX Rights Administration	Bearbeitung der Exchange-Berechtigungsstufen.	System
2022	Find Department Approvers	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	
8055	License Pool Analysis	Nutzung der Analysefunktion für Lizenz-Pools.	System
8054	License Pool List	Verwaltung der Lizenz-Pools.	System
8222	Manage Active Directory Categories	Verwaltung der Active Directory-Kategorien.	System
8035	Manage Active Directory Domains	Verwaltung der Active Directory-Domänen.	System

8220	Manage Active Directory Groups	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	
9203	Manage Alert Delivery Modes	Verwaltung der Benachrichtigungskanäle.	System
9202	Manage Alert Subscriptions	Verwaltung der Benachrichtigungen.	System
9100	Manage Antivirus	Einstellung der Antivirus-Software zur Prüfung hochgeladener Dateien.	System
7031	Manage Application Prov. Config.	Erlaubt es, Anwendungsberechtigungen innerhalb von Ressourcen zu verwalten.	System
1100	Manage Approval Contexts	Verwaltung der Kontexte für Genehmigungsworkflows.	
1110	Manage Approval Workflows	Verwaltung der Genehmigungsworkflows.	System
8100	Manage Budget Periods	Wartung der Budgetperioden.	System
8037	Manage Buildings	Verwaltung der Gebäude.	System
8092	Manage Certificates	Verwaltung der Zertifikate.	System
8033	Manage Companies	Verwaltung der Unternehmen.	System
8036	Manage Cost Centers	Verwaltung der Kostenstellen.	System
8085	Manage Credentials	Verwaltung der Zugangsdaten.	System
8235	Manage Data Owner Successors	Nutzung der Nachfolger-Funktion für Dateneigentümer.	System
8022	Manage Department Groups	Verwaltung der Abteilungsgruppen.	System
8023	Manage Department Owners	Festlegen der Abteilungsverantwortlichen.	System
3201	Manage Directory Templates	Verwaltung der Verzeichnisvorlagen.	System
8096	Manage Email Rules	Verwaltung der Regeln zur Erzeugung von E-Mail-Adressen.	System
8333	Manage Exchange Groups	Erlaubt den Import bestehender Exchange-Berechtigungsgruppen.	System

8012	Manage EXECs	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	
8093	Manage Field Mappings	Verwaltung der Feldmappings.	System
8097	Manage Field Rules	Verwaltung der Feldregeln.	System
8091	Manage Fileserver Group Configuration	Bearbeiten der Fileserver-Gruppenkonfiguration.	System
8321	Manage Fileserver Groups	Verwaltung der Einstellungen, welche Gruppe für welches Verzeichnis und welche Berechtigungsstufe verantwortlich ist.	System
8210	Manage Fileserver Privilege Levels	Verwaltung der Fileserver-Berechtigungsstufen.	System
8270	Manage Fileserver Scans	Anzeige der Scanvorgänge.	System
1123	Manage Genders	Geschlechterverwaltung.	System
8015	Manage HTTP Interfaces	Verwaltung der HTTP-Interfaces.	System
8013	Manage Jobs	Jobverwaltung.	System
8300	Manage Languages	Verwaltung der Sprachen.	System
9210	Manage License	Erlaubt die Verwaltung der Lizenz-Einstellungen.	
1124	Manage Lifecycle Phases	Verwaltung der Lifecycle-Phasen.	System
9130	Manage Office 365 Team Templates	Verwaltung der Teams-Vorlagen.	System
8350	Manage Microsoft 365 Tenants	Verwaltung der Microsoft 365 Mandanten.	System
8032	Manage Offices	Verwaltung der Niederlassungen.	System
8034	Manage Organization Unit Groups	Verwaltung der Organisationseinheitsgruppen.	System
8089	Manager Parameters	Verwaltung der möglichen Parameter.	System
8086	Manage Password Policy	Verwaltung der Passwort-Policies.	System
2090	Manage Person Links	Verwaltung der Personenverknüpfungen.	System

8014	Manage Person Lists	Verwaltung von Personenlisten.	System
1119	Manage Person Type Links	Verwaltung der Personenart-Verknüpfungen.	System
1120	Manage Person Types	Verwaltung der Personenarten.	System
8084	Manage Phone Systems	Verwaltung der Telefonanlagen.	System
8400	Manage Plugins	Verwaltung der Plugins.	System
1122	Manage Positions	Verwaltung der Positionen (Personen).	System
7030	Manage Privileges (tenfold)	Verwaltung der tenfold-Berechtigungen (die aktuell beschriebene Funktion).	System
3071	Manage Profile Auto Align Rules	Verwaltung der Einstellungen für den automatischen Profilabgleich.	System
8070	Manage Profiles	Verwaltung der Profile.	System
8450	Manage Provisioning Conditions	Verwaltung der Bedingungen.	System
8311	Manage Recertification Policies	Verwaltung der Rezertifizierungsrichtlinien.	System
3200	Manage Report Templates	Verwaltung der Berichtsvorlagen.	System
1140	Manage Request Reasons	Verwaltung der Request-Gründe.	System
8053	Manage Resource Options	Verwaltung der Optionen (Ressourcen).	System
8083	Manage Scripts	Verwaltung der Scripts.	System
8342	Manage SharePoint Groups	Import der SharePoint-Berechtigungsgruppen.	System
8600	Manage SMTP-Server	Verwaltung der Einstellungen für den E-Mail-Versand.	System
8011	Manage Templates	Verwaltung der E-Mail-Vorlagen.	System
8280	Manage tenfold Agents	Verwaltung der tenfold-Agents.	System
1121	Manage Titles	Verwaltung der Titel (Personen).	System

8501	Manage Two Factor Authentication (OTP key)	Verwaltung der gespeicherten Token für OTP-Anmeldung.	System
8095	Manage UPN Rules	Verwaltung der Regeln zur Erzeugung von User Principal Names.	System
8094	Manage Username Rules	Verwaltung der Generatoren für Benutzernamen.	System
8087	Manage Verifications Policies	Verwaltung der Verifizierungsrichtlinien.	System
8040	Mappings Administration	Verwaltung der CMDB- und Kostenstellenzuordnungen.	System
1040	Move to other department	Nutzung der Funktion "Abteilungswechsel".	Organisation
1041	Move to other department suggestion	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	Organisation
8030	Organization Unit Administration	Verwaltung der Organisationseinheiten.	System
3092	Profile Preview	Verwendung der Funktion "Profilabgleich".	System
4010	Quick Search for Deleted Person	Erlaubt es, bei der Schnellsuche auch nach gelöschten Personen zu suchen.	System
3102	Report Active Directory	Verfügbarkeit der Option "Active Directory" beim Bericht zu einer Person.	System
3104	Report Exchange Server	Verfügbarkeit der Option "Exchange Server" beim Bericht zu einer Person.	System
3100	Report Fileserver	Verfügbarkeit der Option "Fileserver" beim Bericht zu einer Person.	System
9220	Report Microsoft 365	Verfügbarkeit der Option "Microsoft 365" beim Bericht zu einer Person.	System
3108	Report Resource Assignments	Verfügbarkeit der Option "Ressourcen" beim Bericht zu einer Person.	System
3106	Report SharePoint Server	Verfügbarkeit der Option "SharePoint" beim Bericht zu einer Person.	System
2010	Request Service / PM Changes	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	

9201	Reset Alert Notification Status	Erlaubt das Zurücksetzen des Status einer Benachrichtigung, wenn diese zu oft fehlgeschlagen ist.	System
8800	REST API administration	Verwaltung der REST-API-Keys.	System
7020	Role Definition	Verwaltung der tenfold-Rollen und deren Zuordnungen.	System
2030	Search List	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	
2111	Self service delete all other resources	Erlaubt es, im Self-Service Ressourcen-Zuordnungen anderer Personen zu entfernen.	Organisation
2110	Self service delete all own resources	Erlaubt es, im Self-Service Ressourcen-Zuordnungen der eigenen Person zu entfernen.	System
2100	Self Service Request Own Resources	Nutzung des Self-Services für die eigene Person.	System
8056	Service Data Owners	Festlegen von Dateneigentümern bei Ressourcen.	System
8052	Service Request Retry	Wiederholung von fehlgeschlagenen Requests.	System
8050	Service Administration	Verwaltung der Ressourcen.	System
8260	Set Data Owner	Erlaubt das Setzen von Dateneigentümern auf Fileserver-Verzeichnissen.	System
8261	SetDataOwnerForExchangeMailboxes	Erlaubt das Setzen von Dateneigentümern auf Exchange-Servern.	System
8340	SharePoint Resource Group Configuration Administration	Konfiguration der Einstellung zur Erzeugung von Berechtigungsgruppen für Exchange.	System
8500	Two Factor Authentication	Benutzer, denen diese Berechtigung zugeordnet ist, müssen bei der Anmeldung ihr Einmalpasswort (OTP) eingeben.	System
8114	Upload My Person Picture	Erlaubt das Hochladen eines Bildes für die eigene Person.	System
8112	Upload Person Picture	Erlaubt das Hochladen von Bildern für Personen.	System
3020	Use Auditor	Verwendung der Auditor-Funktion.	Organisation
3012	Use Bulk Change	Verwendung der Funktion "Massenänderung".	System
8290	Use Dashboard	Verwendung des Dashboards.	System

9120	Use Maintenance Mode	Erlaubt die Anmeldung, während der Wartungsmodus aktiv ist.	System
2021	Use Person Search (Default)	Verwendung der Personensuche mittels Standardfiltern.	System
2032	Use Person Search (Field Rules)	Verwendung der Personensuche mittels Feldregeln.	System
3080	Use Profile Assistant	Verwendung des Profilassistenten.	Organisation
3081	Use Profile Assistant with Field Rule Search	Erlaubt die Verwendung des Profilassistenten mit Feldregeln.	System
2024	Use Quick Search	Verwendung der Schnellsuche.	System
2029	Use Quick Search for Active Directory	Schnellsuche für Active Directory-Objekte.	System
2027	Use Quick Search for Exchange Server	Schnellsuche für Exchange-Objekte.	System
2026	Use Quick Search for Fileservers	Schnellsuche für Verzeichnisse auf dem Fileserver.	System
2031	Use Quick Search for Microsoft 365 Objects	Schnellsuche für Objekte (Gruppen, Benutzer, etc) auf Microsoft 365 Mandanten.	System
2028	Use Quick Search for SharePoint	Schnellsuche für SharePoint-Objekte.	System
3110	Use Scan on entire Fileserver	Scan eines gesamten Fileservers über die Fileserver-Administration starten.	System
3111	Use Scan on Single Directory	Scan eines einzelnen Verzeichnisses über die Fileserver-Administration starten.	System
1000	Use System (Basic Login Privilege)	Erlaubt die grundsätzliche Verwendung des Systems. Ohne diese Berechtigung ist eine Anmeldung nicht möglich.	System
8700	User Account Selection Rules administration	Verwaltung der Regeln für die Account-Zuordnung.	System
8060	Value Group Configuration Admin.	Verwaltung der Nachschlagewerte	System
8223	Use Active Directory Pathfinder	Verwendung des Pathfinders.	System

9000	View Activities	Anzeige der Aktivitäten.	System
3019	View Activity Requests	Anzeige der Requests auf der Aktivitätsliste.	System
9024	View Alerts	Anzeige der Benachrichtigungen.	System
3016	View all Events	Anzeige aller Ereignisse.	System
2060	View Assignments	Anzeige der Zuordnungen von Ressourcen.	Organisation
1130	View Cost Allocation	Anzeige der Kostenzuordnung (nur wirksam, wenn die Finanzfunktion aktiviert ist).	System
8081	View Current Sessions	Anzeige der aktuellen Benutzersessions.	System
8230	View Data Owners	Nutzung der Übersichtsfunktion für Dateneigentümer.	System
8021	View Department	Anzeige der Details zu Abteilungen.	System
8650	View Email Log	Anzeige der Mail-Historie.	System
3015	View Events in Requests	Anzeige der Ereignisse innerhalb eines Requests.	Organisation
8332	View Exchange Groups	Anzeige der Exchange-Berechtigungsgruppen.	System
3017	View EXECs in Requests	Anzeige der ausgeführten Scripts innerhalb eines Requests.	Organisation
1022	View Expired Persons	Anzeige der bald ablaufenden und bereits abgelaufenen Personen (im Genehmigungsbereich).	System
1023	View Expired Resources	Anzeige der bald ablaufenden und bereits abgelaufenen Ressourcen (im Genehmigungsbereich).	System
8320	View Fileserver Groups	Nutzung der Funktion "Verwendete Fileservergruppen".	System
3018	View Future Events	Anzeige der zukünftigen Änderungen.	System
3011	View Future Requests	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	System
8016	View Job History	Anzeige der Job-Historie.	System
1021	View Locked Persons	Anzeige der bereits gesperrten Personen (im Genehmigungsbereich).	System
1024	View Locked Resources	Anzeige der bereits gesperrten Ressourcen (im Genehmigungsbereich).	System

2025	View My Data	Anzeige der eigenen Stammdaten.	System
8313	View My Recertifications	Anzeige der Rezertifizierungen, welche man selbst durchgeführt hat.	System
3013	View My Requests	Anzeige der Requests, die man selbst erstellt hat sowie jene, die man selbst genehmigt hat.	System
8031	View Organization Unit	Anzeige der Organisationseinheiten.	System
8088	View Password Reset Log	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte. (abgelöst durch tenfold Auditor)</i>	System
2050	View Person	Anzeige von Personen.	Organisation
2080	View Person Expert Mode	Steuert, ob der Karteireiter "Ressourcen" (nur lesend) angezeigt wird.	System
3014	View Processing Requests	Anzeige der Requests, welche aktuell durchgeführt werden.	System
3030	View Profile	Anzeige der aktuell und historisch zugeordneten Profile sowie Abweichungen zu einer Person.	Organisation
3060	View Profile Assignments	Verwendung der Maske "Profilzuordnungen".	Organisation
3070	View Profile Deviations	Anzeige der Profilabweichungen.	Organisation
8310	View Recertifications	Anzeige der aktuellen und historischen Rezertifizierungsprozesse, inklusive Detailinformationen.	System
3006	View Requests for Active Directory	Anzeige von Requests mit dem Modus "Active Directory" in der Request-Liste.	System
3008	View Requests for Application Priv.	Anzeige von Requests mit dem Modus "Anwendungsberechtigung" in der Request-Liste.	Organisation
3000	View Requests for Data Corrections	Anzeige von Requests mit dem Modus "Datenkorrektur" in der Request-Liste.	Organisation
3003	View Requests for Exchange Server	Anzeige von Requests mit dem Modus "Exchange-Server" in der Request-Liste.	System
3005	View Requests for Fileserver	Anzeige von Requests mit dem Modus "Fileserver" in der Request-Liste.	System

2999	View Requests for Lifecycle	Anzeige von Requests mit dem Modus "Lifecycle" in der Request-Liste.	Organisation
2998	View Requests for Microsoft 365 Groups	Anzeige von Requests für Microsoft 365 Objekte.	System
2997	View Requests for Microsoft 365 Licenses	Anzeige von Requests für Microsoft 365 Lizenzen.	System
2996	View Requests for Office 365 Teams	Anzeige von Requests für Microsoft 365-Teams.	System
3001	View Requests for Passwords	Anzeige von Requests mit dem Modus "Passwort" in der Request-Liste.	Organisation
3010	View Requests for Person Changes	Anzeige von Requests mit dem Modus "Personendaten" in der Request-Liste.	Organisation
3007	View Requests for Person Changes (Resource)	Anzeige von Requests mit dem Modus "Personendaten" (bei Nutzung mehrerer Personendatensätze) in der Request-Liste.	Organisation
3002	View Requests for Profile Alignment	Anzeige von Requests mit dem Modus "Profil" in der Request-Liste.	Organisation
3009	View Requests for Resource Assignments	Anzeige von Requests mit dem Modus "Ressource" in der Request-Liste.	Organisation
3004	View Requests for SharePoint Server	Anzeige von Requests mit dem Modus "SharePoint" in der Request-Liste (Hinweis: aktuell noch nicht in Verwendung).	System
9110	View Security Dashboard	Verwendung des Security-Dashboards.	System
8051	View Service Masterdata	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	
8341	View SharePoint Groups	Anzeige der verwendeten SharePoint-Berechtigungsgruppen.	System
8082	View System Information	Anzeige der Systeminformationen.	System
8325	View Temporarily Locked Active Directory Users	Anzeige der gesperrten Active Directory-Konten (Sperrung durch mehrfache Eingabe eines falschen Passworts).	System
8250	View User Name Suggestion	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>	

View Requests

Einige der "View Requests for X"-Berechtigungen waren bis Version tenfold 2022 R1 Update 3 als Systemberechtigung gekennzeichnet. Dies hatte zur Folge, dass mit einer der Berechtigungen alle Requests des jeweiligen Typs angezeigt wurden, unabhängig von Einschränkungen in den Rollenzuweisungen. Für Installationen ab Version tenfold 2022 R1 Update 3 werden diese nun als organisationsabhängige Berechtigungen geführt. Bitte beachten Sie, dass ein Update von älteren Versionen auf eine Version ab tenfold 2022 R1 Update 3 diese Einstellungen **nicht** verändert, da dies zu unvorhergesehenen Änderungen Ihres Berechtigungsmodells führen kann. Um die Berechtigungseinstellungen zu ändern, benutzen Sie das unten angeführte SQL-Skript, sollten Sie diese Berechtigungen auf organisatorischer Ebene einschränken wollen.

Update der View Request-Berechtigungen

```
-- Update 'View Requests for Lifecycle'
UPDATE PRIVILEGE SET PTYPE = 'D' WHERE ID = 2999;

-- Update 'View Requests for Data Corrections'
UPDATE PRIVILEGE SET PTYPE = 'D' WHERE ID = 3000;

-- Update 'View Requests for Passwords'
UPDATE PRIVILEGE SET PTYPE = 'D' WHERE ID = 3001;

-- Update 'View Requests for Profile Alignment'
UPDATE PRIVILEGE SET PTYPE = 'D' WHERE ID = 3002;

-- Update 'View Requests for Person Changes (Resource)'
UPDATE PRIVILEGE SET PTYPE = 'D' WHERE ID = 3007;

-- Update 'View Requests for Application Privileges'
UPDATE PRIVILEGE SET PTYPE = 'D' WHERE ID = 3008;

-- Update 'View Requests for Resource Assignments'
UPDATE PRIVILEGE SET PTYPE = 'D' WHERE ID = 3009;

-- Update 'View Requests for Person Changes'
UPDATE PRIVILEGE SET PTYPE = 'D' WHERE ID = 3010;
```

12.6 Zwei-Faktor-Authentifizierung (2FA)

12.6.1 Zweck

Die Zwei-Faktor-Authentifizierung (siehe dazu auch <https://de.wikipedia.org/wiki/Zwei-Faktor-Authentisierung>) dient dazu, die Anmeldung an tenfold sicherer zu gestalten. Besonders bei konfiguriertem Single Sign On (SSO; siehe [Einrichten von Single Sign On](#) (see page 441)) verhindert die 2FA, dass eine Person ein ungesperstes Endgerät übernimmt und anschließend tenfold ohne weitere Authentifizierung nutzen kann. Zusätzlich kann die 2FA auch in Workflows genutzt werden. Wenn für einen Workflow-Schritt 2FA

konfiguriert ist, so muss der Benutzer bei der Freigabe des Workflows seinen Passkey eingeben - ansonsten ist die Freigabe nicht möglich (siehe auch [Workflows](#)(see page 380)).

12.6.2 Funktionsweise

Die 2FA in tenfold wird über das Verfahren OATH-TOTP realisiert. Das Verfahren basiert im Kern auf einer kryptografischen Hash-Funktion HMAC, mit deren Hilfe aus dem zwischen Sender und Empfänger vereinbarten und geheimen Schlüssel K und der absoluten Uhrzeit ein kryptografischer Hash-Wert berechnet wird. Dazu wird die Uhrzeit in einen ganzzahligen Sekundenwert gewandelt, üblicherweise werden dabei die Anzahl der Sekunden seit 1. Januar 1970 herangezogen, und dieser Wert auf eine Schrittweite von 30 Sekunden gerundet. Das Einmalkennwort ist innerhalb dieser Dauer von 30 Sekunden gültig. Je nach konkreter Implementierung und Konfiguration werden auch noch die zeitlich benachbarten Intervalle akzeptiert. Wesentlich bei diesem Verfahren ist, dass die beiden Systeme, Sender und Empfänger, über hinreichend genaue Uhren oder über einen Zugang wie dem Network Time Protocol (NTP) zu einer genauen Uhrzeitinformation verfügen müssen, da andernfalls die Authentifizierung fehlschlägt (Quelle: Wikipedia). Für das Verfahren stehen mehrere Apps für mobile Geräte zur Verfügung:

App	iPhone (iOS)	Android
Google Authenticator	VERFÜGBAR	VERFÜGBAR
Microsoft Authenticator	VERFÜGBAR	VERFÜGBAR
Sophos Authenticator	VERFÜGBAR	VERFÜGBAR

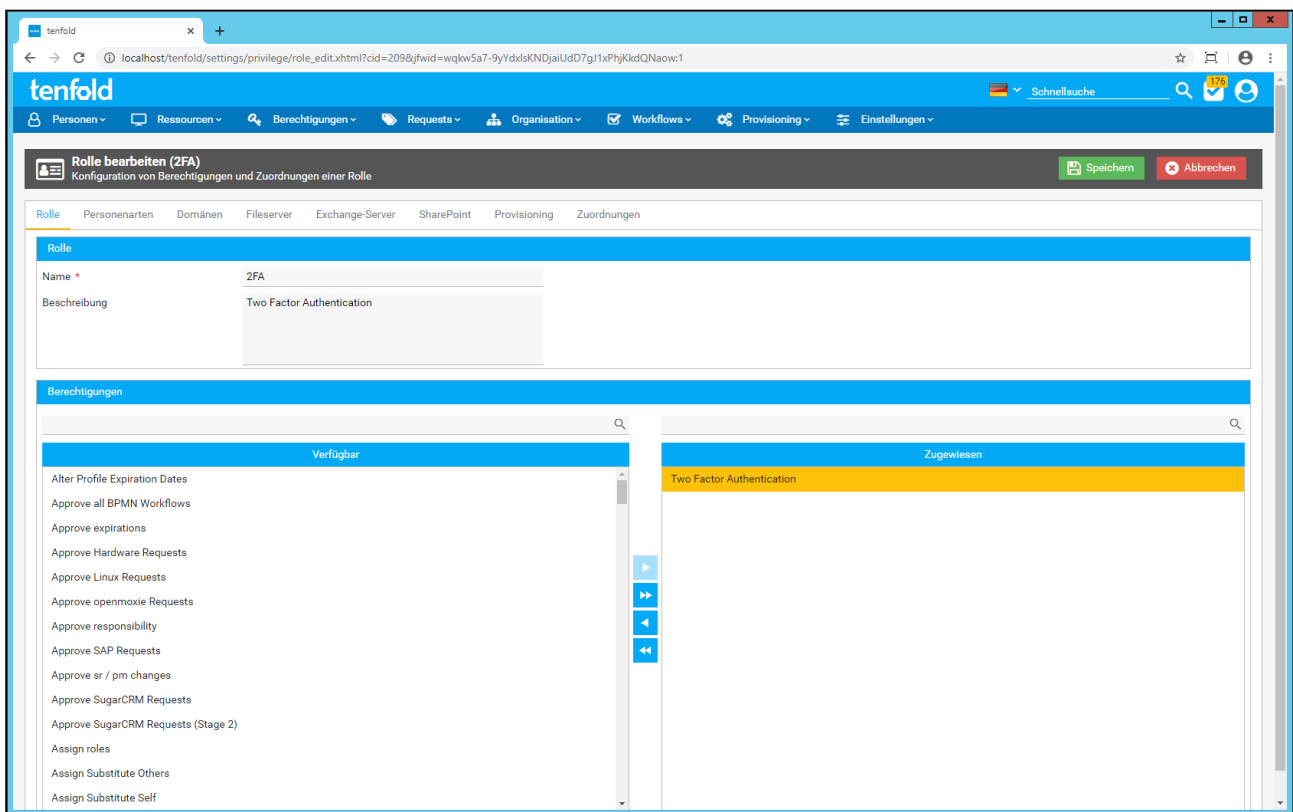
12.6.3 Konfiguration

Die Konfiguration von 2FA läuft in zwei Schritten ab:

- Festlegen, für welche Benutzer 2FA zur Anwendung kommt
- Individuelle Einrichtung durch die einzelnen Benutzer

12.6.4 Benutzer festlegen

Für welche Benutzer die 2FA gilt, wird über eine tenfold Berechtigung gesteuert (siehe [Berechtigungen](#)(see page 457)). Ist einem Benutzer die Systemberechtigung "Two Factor Authentication" (8500) zugeordnet, so ist für diesen Benutzer 2FA aktiviert und verpflichtend.

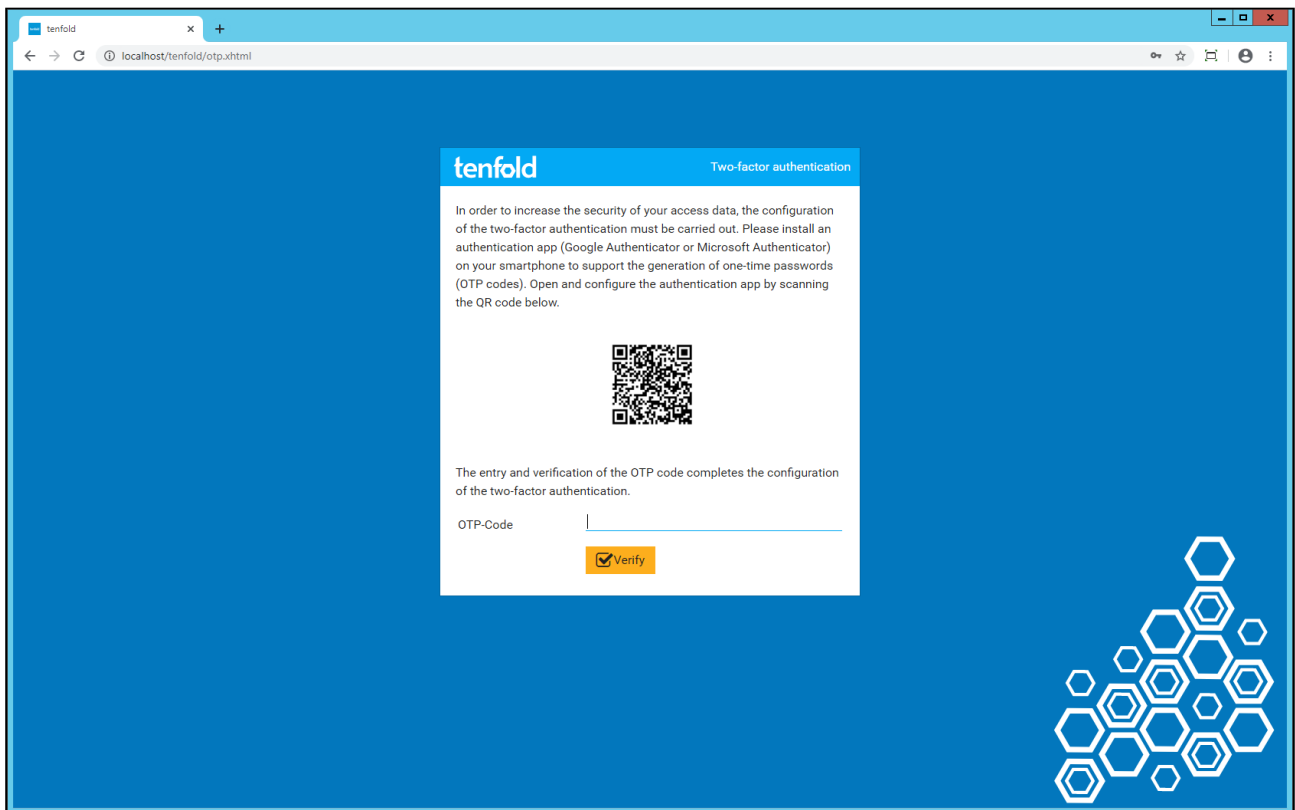


Warnung

Die Aktivierung von 2FA ist sowohl für den Authentifizierungsmodus "SSO" als auch für den Modus "Form" verfügbar (siehe [Einrichten von Single Sign On](#) (see page 441)). 2FA sollte nicht verwendet werden, so lange sich das System noch im Modus "Setup" befindet.

12.6.5 Benutzerkonfiguration

Sobald sich ein Benutzer, dem 2FA über die entsprechende Systemberechtigung zugeordnet wurde, das nächste Mal anmeldet, muss erhält er einen Hinweis mit einem QR-Code. Dieser beinhaltet den HMAC-Code, der für die Generierung der Einmalpassworte erforderlich ist. Der QC-Code muss mit der App (siehe oben) eingescannt werden und liefert anschließend laufend Einmalpassworte (diese rotieren alle 30 Sekunden) die in der App abgelesen werden können. Zur Bestätigung muss das aktuelle OTP (Einmalpasswort) eingegeben werden. Anschließend wird der Benutzer angemeldet. In weiterer Folge muss der Benutzer das OTP bei jeder Anmeldung in einem separaten Schritt eingeben.

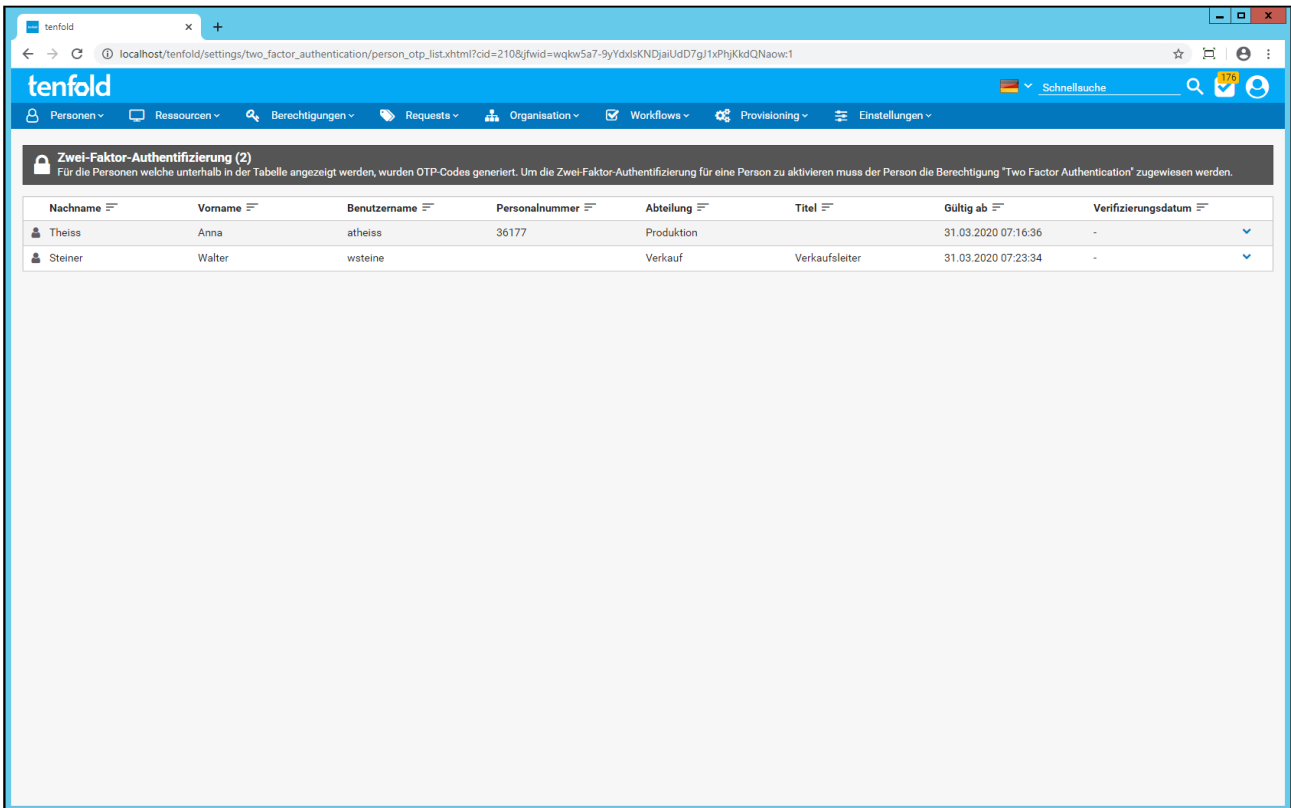


12.6.6 Token-Verwaltung

Über das Menü "Einstellungen > Zwei-Faktor-Authentifizierung" können die aktuell ausgestellten Tokens (HMAC-Codes) angezeigt werden. Über das Kontextmenü kann ein Eintrag wieder gelöscht werden. Das hat zur Folge, dass der Benutzer bei der nächsten Anmeldung erneut einen QR-Code scannen muss. Der neue QR-Code hat keine Verbindung zum gelöschten Eintrag. Eine Anmeldung mit einem OTP von einem gelöschten Eintrag ist nicht möglich.

Benötigte Berechtigung

Für diese Funktion ist die Systemberechtigung "Manage Two Factor Authentication (OTP key)" (8501) erforderlich.



Zwei-Faktor-Authentifizierung (2)
Für die Personen welche unterhalb in der Tabelle angezeigt werden, wurden OTP-Codes generiert. Um die Zwei-Faktor-Authentifizierung für eine Person zu aktivieren muss der Person die Berechtigung "Two Factor Authentication" zugewiesen werden.

Nachname	Vorname	Benutzername	Personalnummer	Abteilung	Titel	Gültig ab	Verifizierungsdatum
Theiss	Anna	atheiss	36177	Produktion		31.03.2020 07:16:36	-
Steiner	Walter	wsteine		Verkauf	Verkaufsleiter	31.03.2020 07:23:34	-

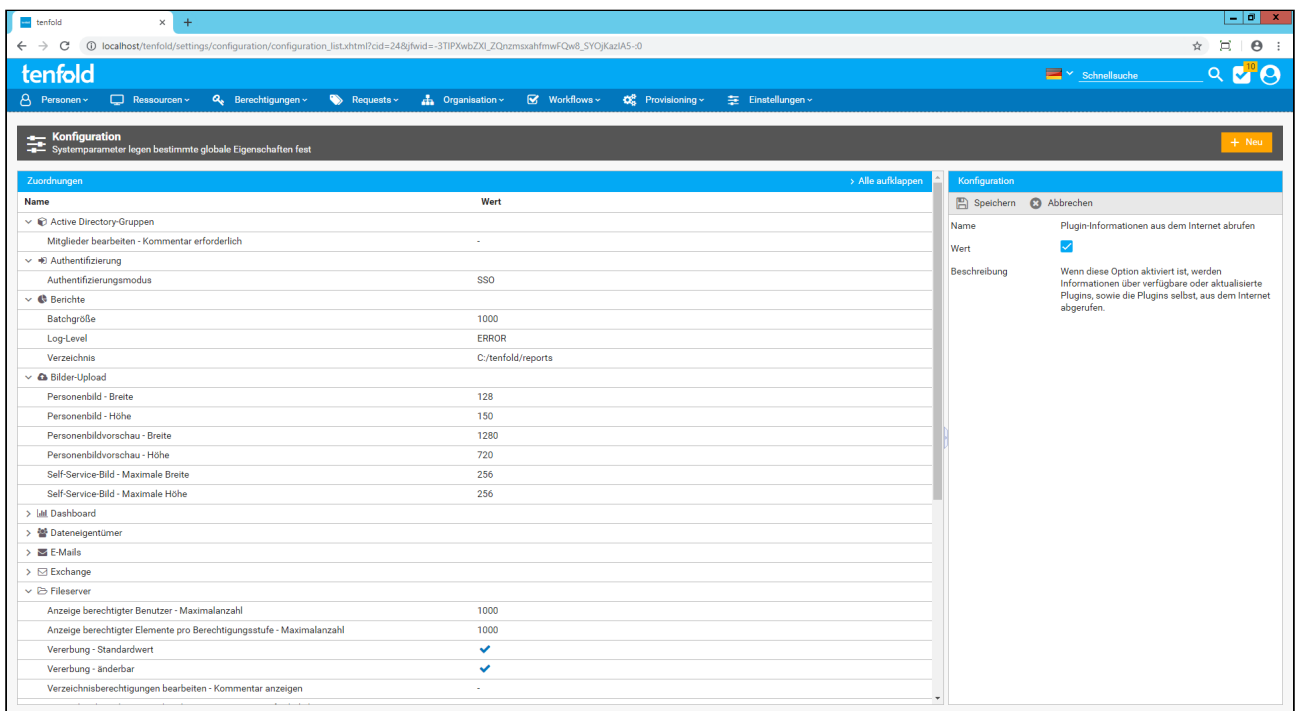
Tip

Sollte ein Benutzer sein Endgerät verlieren oder dieses aufgrund Beschädigung nicht mehr verwendbar sein, nutzen Sie diese Funktion um die Anmeldung mit einem alten OTP zu verhindern und dem Benutzer die Möglichkeit zu geben, die Einrichtung erneut durchzuführen.

12.7 Systemparameter

Hinweis

Systemparameter sollten nur geändert werden, wenn man sich ganz sicher über die Auswirkung der Änderung ist. Falsch eingestellte Parameter können zu Fehlverhalten und Datenverlust führen.



12.7.1 Allgemeines

Systemparameter steuern das Verhalten von tenfold auf globaler Ebene. Systemparameter sind vom Kontext unabhängig, gelten für jeden Benutzer und in jeder Situation (Ausnahmen sind gegebenenfalls unterhalb beschrieben). Ein Systemparameter hat einen bestimmten Namen und einen zugeordneten Wert. Darüber hinaus kann im Feld Beschreibung eine Erläuterung zum Zweck des Parameters hinterlegt werden. Es wird zwischen zwei verschiedenen Typen von Parametern unterschieden.

Parameter für Ressourcen/Personenarten

Verwechseln Sie die Systemparameter nicht mit den Parametern, welche Sie bei Ressourcen und Personenarten hinterlegen können. Diese finden Sie im Menü unter Provisioning > Parameter und stehen in keinem Zusammenhang zu den Systemparametern.

Standardparameter

Diese sind im Auslieferungszustand des Systems bereits vorhanden. Es kann lediglich der Wert angepasst werden, der Name kann nicht verändert werden. Jeder Standardparameter verfügt über eine Beschreibung, die angibt, welches Verhalten mit dem Parameter kontrolliert wird. Je nach Parameter können diese als Freitext, Auswahlliste oder Checkbox bearbeitet werden.

Neustart

Für die Änderung mancher Systemparameter ist ein Neustart des tenfold-Dienstes notwendig, damit die Änderung wirksam wird. In der Beschreibung des jeweiligen Parameters werden Sie darauf hingewiesen ob es für diesen der Fall ist.

Benutzerdefinierte Parameter

Es ist möglich neue Parameter zum System hinzuzufügen. Diese dienen primär dazu, um das Verhalten von selbst entwickelten EXECs (Funktionsbausteinen) steuern zu können. Es können sowohl der Name als auch der Wert angepasst werden. Ein Systemparameter kann als Parameter für Skripte der Groovy- oder PowerShell-Plugins verwendet werden. Sie können diese Möglichkeit nutzen um Werte, welche in mehreren Provisionierungsschritten dieser Plugins verwendet werden, zentral zu verwalten.

Passworte

Die Systemparameter eignen sich nicht dazu, die Zugangsdaten (Verbindung, Benutzer, Passwort und ähnliches) für eine Zielapplikation zu hinterlegen. Die Systemparameter werden in der Datenbank nicht verschlüsselt gespeichert. Wenn Sie Benutzer und/oder Passworte hinterlegen wollen, nutzen Sie stattdessen die Funktion zum Hinterlegen von Zugangsdaten (Menü > Provisioning > Zugangsdaten).

Benutzerdefinierte Systemparameter werden immer als Freitextfelder behandelt. Auswahllisten oder Checkboxes wie bei diversen Standardparametern sind nicht möglich.

Beschreibung

Verwenden Sie die Beschreibung des Systemparameters um zu dokumentieren, an welchen Stellen Ihr benutzerdefinierter Parameter verwendet wird.

12.7.2 Verwaltung von Systemparametern

Benötigte Berechtigung

Für die Verwaltung ist die Berechtigung "Configuration administration" (8010) erforderlich.

Die Liste der Systemparameter kann unter Menü > Einstellungen > System > Parameter angezeigt werden. Mit dem Hinzufügen-Button kann ein neuer, benutzerdefinierter Eintrag angelegt werden. Um einen bestehenden Systemparameter zu bearbeiten, wählen Sie diesen aus und bearbeiten dessen Wert (Textfeld, Checkbox oder Dropdown-Liste) im rechten Teil der Maske. Mit der Schaltfläche "Speichern" können Sie den neuen Wert abspeichern.





Auswahl ändern

Wenn Sie einen anderen Systemparameter auswählen, ohne vorher die Änderungen zu speichern, gehen Ihre Änderungen verloren.

12.7.3 Liste der Standardparameter

Im folgenden finden Sie eine Auflistung und Beschreibung der Standardparameter.







Parameter	Beschreibung	Typ	Neustart
> Active Directory-Gruppen			

Active Directory-Gruppen mit PowerShell verwalten	Um Konten aus Domäne zu Mitgliedern von Gruppen aus anderen vertrauenswürdigen Domänen machen zu können, müssen in der Domäne der Gruppe zuerst sogenannte Foreign Security Principals angelegt werden. In früheren Versionen von tenfold wurde dies durch den Aufruf eines PowerShell-Skriptes erledigt. Neuere Versionen von tenfold verwalten diese direkt über die LDAP-Schnittstelle des Active Directory. Dies ist schneller als der Aufruf des PowerShell-Skriptes. Sollten Sie dennoch die ältere Variante weiterhin verwenden wollen, aktivieren Sie diese Einstellung.	Checkbox	
E-Mail-aktivierte Gruppen umbenennen - Aktiviert	Das Umbenennen von E-Mail-aktivierten Active Directory-Gruppen, erfordert zusätzliche Eingriffe in Exchange, welche von tenfold nicht durchgeführt werden. Daher ist das Umbenennen dieser Gruppen deaktiviert. Mit dieser Einstellung können Sie das Umbenennen für E-Mail-aktivierte Gruppen aktivieren. Achtung: tenfold führt weiterhin keine Anpassungen in Exchange durch, wenn die Gruppen umbenannt werden. Diese müssen durch eine benutzerdefinierte Provisionierung bereitgestellt werden.	Checkbox	
Mitglieder bearbeiten - Kommentar erforderlich (Self-Service)	Legt fest, ob der Request-Kommentar auf der Self-Service-Maske zum Bearbeiten von Gruppenmitgliedern erforderlich ist.	Checkbox	
> Aktivitäten			
"Meine Aktivitäten" sichtbar	Steuert, ob die Kachel "Meine Aktivitäten" auf der Startseite oder die Kategorie "Meine Aktivitäten" im Benachrichtigungsmenü neben der Schnellsuche angezeigt werden. Diese werden normalerweise dann angezeigt, wenn dem angemeldeten Benutzer Aktivitäten zur Bearbeitung zugeordnet sind. Achtung: Ist diese Einstellung deaktiviert, ist die einzige Möglichkeit über offene Aktivitäten informiert zu werden mittels eine E-Mail-Nachricht. Andernfalls muss der Benutzer selbstständig in tenfold die Aktivitätsliste prüfen, sofern dieser dazu Berechtigt ist.	Checkbox	
> Authentifizierung			

Anmeldeversuche - Anmeldung deaktiviert	<p>Legt die Zeit nach einem fehlgeschlagenem Anmeldeversuch fest, welche der Benutzer warten muss, bevor ein neuer Anmeldeversuch stattfinden kann. Diese Einstellung muss zwingend als 4 kommasetrennte Zahlen hinterlegt werden. Diese Zahlen legen den Wert in Sekunden fest, welche der Benutzer nach:</p> <ol style="list-style-type: none"> 1. 3 Versuchen 2. 5 Versuchen 3. 10 Versuchen 4. 20 Versuchen <p>warten muss, bevor eine neue Anmeldung stattfinden kann.</p>	Text	✓
Authentifizierungsmodu s	<p>Legt fest, wie sich Benutzer in tenfold anmelden können.</p> <ul style="list-style-type: none"> • Form: Benutzer melden sich über ein Anmeldeformular mit deren Windows-Benutzernamen und Passwort an. • Setup: Benutzer werden automatisch als der Systembenutzer "systemfold" angemeldet. Diese Einstellung ist nur für initiale Einrichtungen gedacht, bis regulären Benutzern die erforderlichen Rollen zugewiesen wurden. • SSO: Die Anmeldung erfolgt mittels Single-Sign-On. Der Benutzer muss keine Anmeldedaten eingeben, sondern wird direkt mit dem angemeldeten Windows-Benutzer an tenfold angemeldet. Single-Sign-On wird nur mittels Kerberos unterstützt. 	Auswahl	✓
Gleichzeitige Anmeldung deaktivieren	Ist diese Einstellung aktiv, wird die Anmeldung eines Benutzers verhindert, wenn es zu diesem Benutzer bereits von einem anderen Gerät eine laufende Session gibt.	Checkbox	✗
> Benachrichtigungen			
Anzahl der Versuche um eine Benachrichtigung zu übermitteln	Die Anzahl an Versuchen, wie oft versucht wird eine Benachrichtigung über einen Kanal zu versenden (siehe Benachrichtigungen (see page 448)), bevor weitere Versuche abgebrochen werden und stattdessen eine weitere Benachrichtigung über den Fehlschlag des Versands erzeugt wird.	Text	✗




Minuten zwischen den Zustellungsversuchen fehlgeschlagener Benachrichtigungen	Eine kommasetrennte Liste von Zahlen, welche die Anzahl von Minuten darstellt, welche zwischen den einzelnen fehlgeschlagenen Versandversuchen einer Benachrichtigung verstreichen, bevor der nächste Versuch unternommen wird. Sollten weniger Werte in der Liste vorhanden sein, als Zustellungsversuche unternommen werden, so wird der letzte Eintrag der Liste für alle weiteren Versuche verwendet.	Text	✗
> Berichte			
Batchgröße	Legt fest, wie viele Verzeichnisse beim Erstellen eines Fileserver-Berichtes gleichzeitig geladen und geschrieben werden. Höhere Werte steigern die Performance, erhöhen jedoch den Speicherverbrauch während der Erstellung.	Text	✗
Log-Level	Legt den Log-Level fest, ab welchem die Bericht-Engine Log-Statements in ihre Log-Datei schreibt. Folgende Optionen stehen zur Auswahl: <ul style="list-style-type: none"> • Debug • Error • Info • Trace • Warn 	Auswahl	✗
Verzeichnis	Legt das Verzeichnis (auf dem tenfold-Server) fest, in welchem die Bericht-Engine die erzeugten Berichte ablegt.	Text	✗
> Bilder-Upload			
Personenbild - Breite	Die Breite (in Pixel) welche beim Speichern von Personenbildern in tenfold verwendet wird. Das Bild wird nach dem Hochladen vor dem Speichern in diese Größe umgerechnet.	Text	✗
Personenbild - Höhe	Die Höhe (in Pixel) welche beim Speichern von Personenbildern in tenfold verwendet wird. Das Bild wird nach dem Hochladen vor dem Speichern in diese Größe umgerechnet.	Text	✗
Personenbild extern - Breite	Die Breite (in Pixel) welche beim Speichern von Personenbildern in externen Systemen (z.B. Active Directory) verwendet wird. Das Verhältnis von Breite und Höhe des externen Bildes muss dem des in tenfold gespeicherten Bildes entsprechen.	Text	✗

Personenbild extern - Höhe	Die Höhe (in Pixel) welche beim Speichern von Personenbildern in externen Systemen (z.B. Active Directory) verwendet wird. Das Verhältnis von Breite und Höhe des externen Bildes muss dem des in tenfold gespeicherten Bildes entsprechen.	Text	✗
Personenbildvorschau - Breite	Die Breite (in Pixel) welche bei der Vorschau der Bilder in tenfold verwendet wird. Das Seitenverhältnis muss nicht dem des gespeicherten Bildes entsprechen, führt bei Unterschieden jedoch zu einer gestreckten Darstellung.	Text	✗
Personenbildvorschau - Höhe	Die Höhe (in Pixel) welche bei der Vorschau der Bilder in tenfold verwendet wird. Das Seitenverhältnis muss nicht dem des gespeicherten Bildes entsprechen, führt bei Unterschieden jedoch zu einer gestreckten Darstellung.	Text	✗
Self-Service-Bild - Maximale Breite	Die maximale Breite (in Pixel) welche für die Abbildungen von Ressourcen im Self-Service erlaubt ist.	Text	✗
Self-Service-Bild - Maximale Höhe	Die maximale Höhe (in Pixel) welche für die Abbildungen von Ressourcen im Self-Service erlaubt ist.	Text	✗
> Dashboard			
Inaktive Benutzer - Tage	Die Anzahl in Tagen, welche ein Konto ohne interaktive Anmeldung sein muss, damit dieses im Dashboard als inaktives Konto aufscheint.	Text	✗
Verzögerte Anzeige von Active Directory-Informationen	Ist diese Einstellung aktiviert, werden die Informationen über die Anzahl der Probleme der Kacheln von der Kategorie "Active Directory" nicht beim Betreten der Maske geladen. Stattdessen muss erst auf eine Kachel geklickt werden um die entsprechende Information zu bekommen. Verwenden Sie diese Einstellung, wenn das Laden des Dashboards zu lange dauert.	Checkbox	✗
Verzögerte Anzeige von Anforderungsinformationen	Ist diese Einstellung aktiviert, werden die Informationen über die Anzahl der Probleme der Kacheln von der Kategorie "Requests nicht beim Betreten der Maske geladen. Stattdessen muss erst auf eine Kachel geklickt werden um die entsprechende Information zu bekommen. Verwenden Sie diese Einstellung, wenn das Laden des Dashboards zu lange dauert.	Checkbox	✗

Verzögerte Anzeige von Fileserver-Informationen	Ist diese Einstellung aktiviert, werden die Informationen über die Anzahl der Probleme der Kacheln von der Kategorie "Fileserver" nicht beim Betreten der Maske geladen. Stattdessen muss erst auf eine Kachel geklickt werden um die entsprechende Information zu bekommen. Verwenden Sie diese Einstellung, wenn das Laden des Dashboards zu lange dauert.	Checkbox	
Verzögerte Anzeige von Microsoft 365-Informationen	Ist diese Einstellung aktiviert, werden die Informationen über die Anzahl der Probleme der Kacheln von der Kategorie "Microsoft 365" nicht beim Betreten der Maske geladen. Stattdessen muss erst auf eine Kachel geklickt werden um die entsprechende Information zu bekommen. Verwenden Sie diese Einstellung, wenn das Laden des Dashboards zu lange dauert.	Checkbox	
> Datei-Uploads			
>> Bilder			
Bildgröße	Legt die maximal zulässige Größe von Bildern (in Bytes) fest, welche hochgeladen werden kann (Personenbilder, Self-Service-Abbildungen, etc).	Text	
Erlaubte Endungen für Bilder	Legt fest, welche Dateierendungen (z.B. png, gif, etc) beim Hochladen von Bilddateien erlaubt sind. Geben Sie die Endungen als kommagetrennte Liste an und schreiben Sie die Endungen ohne Punkt und ohne Wildcards (z.B. "png" statt ".png" oder "*.png"). Der empfohlene Wert ist: bmp,gif,jpg,jpeg,png	Text	
>> Genehmigungsworkflows			
Dateigröße	Legt die maximal zulässige Größe von Dateien fest, welche als Request-Anhang in Genehmigungsschritten hochgeladen werden kann. Die Größe wird in Bytes angegeben.	Text	
Erlaubte Endungen für Dateianhänge	Legt fest, welche Dateierendungen (z.B. pdf, docx, png) beim Hochladen von Request-Anhängen erlaubt sind. Geben Sie die Endungen als kommagetrennte Liste an und schreiben Sie die Endungen ohne Punkt und ohne Wildcards (z.B. "docx" statt ".docx" oder "*.docx"). Der empfohlene Wert ist: pdf,docx,xlsx,pptx,txt,bmp,gif,jpg,jpeg,png	Text	

Gleichzeitige Anzahl Dateianhänge	Legt die Anzahl an Dateien fest, welche bei Request-Anhängen gleichzeitig hochgeladen werden können.	Text	✗
>> Personendokumente			
Anzahl Personendokumente	Legt fest, wieviele Dokumente zu einer Person hochgeladen werden können.	Text	✗
Erlaubte Endungen für Personendokumente	Legt fest, welche Dateiendungen (z.B. pdf, docx, png) beim Hochladen von Personendokumenten erlaubt sind. Geben Sie die Endungen als kommagetrennte Liste an und schreiben Sie die Endungen ohne Punkt und ohne Wildcards (z.B. "docx" statt ".docx" oder "*.docx"). Der empfohlene Wert ist: pdf,docx,xlsx,pptx,txt,bmp,gif,jpg,jpeg,png	Text	✗
Personendokument-Größe	Legt die maximal zulässige Größe von Personendokumenten (in Bytes) fest.	Text	✗
> Dateneigentümer			
Administratoren als Dateneigentümer anzeigen	Legt fest, ob in den diversen Anzeigen von tenfold, die Mitglieder der Rolle "Administratoren" als Dateneigentümer angezeigt werden soll. Die Mitglieder dieser Rolle erhalten immer automatisch sämtliche Dateneigentümerberechtigungen, es kann jedoch unerwünscht sein, dies den Benutzern darzustellen.	Checkbox	✗
> E-Mails			
Absender-Adresse	Die Standardadresse unter welcher alle E-Mails von tenfold versendet werden.	Text	✗
E-Mails senden	Bestimmt, ob tenfold tatsächlich E-Mails versendet. Ist diese Einstellung deaktiviert, erscheinen gesendete E-Mails nur im Log der gesendeten E-Mails (siehe Historie gesendeter E-Mails (see page 536)). Diese Einstellung ist ident mit der entsprechenden Einstellung auf der Maske der SMTP-Server-Einstellungen (siehe SMTP-Server (see page 532)). Wenn Sie diese Einstellung ändern, wird diese auch auf der SMTP-Server-Maske geändert und umgekehrt.	Checkbox	✗
> Exchange			




Postfachberechtigungen bearbeiten - Kommentar anzeigen	Bestimmt, ob bei der Bearbeitung von Postfachberechtigungen die Eingabe eines Kommentars möglich ist.	Checkbox	✗
Postfachberechtigungen bearbeiten - Kommentar erforderlich	Legt fest, ob bei der Bearbeitung von Postfachberechtigungen die Eingabe eines Kommentars erforderlich ist. Diese Einstellung hat nur dann eine Auswirkung wenn die Einstellung "Postfachberechtigungen bearbeiten - Kommentar anzeigen" aktiv ist.	Checkbox	✗
Postfachgruppen - Größe	Bei der Anzeige der Postfächer auf einem Server, werden die Postfächer nach Namen gruppiert, wenn zu viele Postfächer unterhalb eines Knotens angezeigt werden. Diese Einstellung legt fest, wie viele Postfächer in jeder Gruppierung maximal enthalten sind.	Checkbox	✗
Postfachgruppen - Schwellenwert	Bei der Anzeige der Postfächer auf einem Server, werden die Postfächer nach Namen gruppiert, wenn zu viele Postfächer unterhalb eines Knotens angezeigt werden. Diese Einstellung legt fest, wieviele Postfächer in einem Knoten vorhanden sein müssen, bevor Gruppierungen erzeugt werden.	Checkbox	✗
> Fileserver			
Anzeige berechtigter Benutzer - Maximalanzahl	Die Anzahl der maximal aufgelisteten Benutzer mit Berechtigungen auf einem Verzeichnis auf der Fileserver-Maske. Sind auf einem Verzeichnis mehr Benutzer berechtigt, wird ein entsprechender Hinweis angezeigt und nur eine nach Namen gefilterte Auflistung der Benutzer ist möglich.	Text	✗
Anzeige berechtigter Elemente pro Berechtigungsstufe - Maximalanzahl	Die Anzahl der maximal aufgelisteten Benutzer für eine bestimmte Berechtigungsstufe auf einem Verzeichnis auf der Fileserver-Maske. Sind auf einem Verzeichnis mehr Benutzer berechtigt, wird ein entsprechender Hinweis angezeigt und nur eine nach Namen gefilterte Auflistung der Benutzer ist möglich.	Text	✗
Benachrichtigung vor Ablauf Verzeichnis - Tage	Gibt an, wieviel Tage vor der Löschung eines ablaufenden Verzeichnisses Dateneigentümer oder Administratoren mittels einer E-Mail benachrichtigt werden.	Text	✗

Benutzerdefinierte Scantiefe - Anzahl der Dateien	Hiermit kann eingestellt werden, ob bei Fileservern mit eingeschränkter Scan-Tiefe, dennoch alle Unterverzeichnisse auf die Anzahl der darunterliegenden Dateien und Verzeichnisse gescannt werden. Hinweis: Dies kann sich negativ auf die Performance des Scans auswirken, da die Scan-Tiefe normalerweise eingestellt wird um Dauer des Scans und die gescannte Datenmenge zu optimieren.	Checkbox	
Benutzerdefinierte Scantiefe - Gesamtgröße	Hiermit kann eingestellt werden, ob bei Fileservern mit eingeschränkter Scan-Tiefe, dennoch alle Unterverzeichnisse auf die Dateigröße der darunterliegenden Dateien. Hinweis: Dies kann sich negativ auf die Performance des Scans auswirken, da die Scan-Tiefe normalerweise eingestellt wird um Dauer des Scans und die gescannte Datenmenge zu optimieren.	Checkbox	
DFS - Verzeichnis erstellen aktiv	Normalerweise wird die Anlage neuer Verzeichnisse innerhalb der DFS-Struktur (Ordner zwischen Namespace und Links) unterbunden. Nur auf Ebenen ab DFS-Links ist die Erstellung neuer Verzeichnisse erlaubt. Wird diese Einstellung aktiviert, wird diese Einschränkung aufgehoben und auf der Maske für Fileserver können auch oberhalb von DFS-Links neue Verzeichnisse erstellt werden. Achtung: Die Anlage von Verzeichnissen oberhalb von DFS-Links sollte nur über die DFS-Verwaltung vorgenommen werden. Werden Verzeichnisse über UNC-Pfade angelegt, wie tenfold dies macht, kann dies zu Fehlern mit der Replizierung führen. Sie sollten diese Einstellung nur aktivieren, wenn Sie durch benutzerspezifisches Provisioning (z.B. PowerShell) sicherstellen, dass die Anlage von Verzeichnissen im DFS korrekt durchgeführt wird. Ein solches Provisioning wird von tenfold nicht mitgeliefert.	Checkbox	

DFS - Verzeichnisberechtigungen bearbeiten aktiv.	<p>Normalerweise wird die Bearbeitung von Berechtigungen innerhalb der DFS-Struktur (Ordner zwischen Namespace und Links) unterbunden. Nur auf Ebenen ab DFS-Links ist die Bearbeitung der Berechtigungen erlaubt. Wird diese Einstellung aktiviert, wird diese Einschränkung aufgehoben und auf der Maske für Fileserver können auch oberhalb von DFS-Links die Berechtigungen bearbeitet werden.</p> <p>Achtung: Die Bearbeitung von Berechtigungen oberhalb von DFS-Links sollte nur über die DFS-Verwaltung vorgenommen werden. Werden Berechtigungen über UNC-Pfade bearbeitet, wie tenfold dies macht, kann dies zu Fehlern mit der Replizierung führen. Sie sollten diese Einstellung nur aktivieren, wenn Sie durch benutzerspezifisches Provisioning (z.B. PowerShell) sicherstellen, dass die Vergabe von Berechtigungen im DFS korrekt durchgeführt wird. Ein solches Provisioning wird von tenfold nicht mitgeliefert.</p>		
Fileservergruppen nicht verwenden Option verfügbar	Unter normalen Umständen vergibt tenfold Berechtigungen auf einem Fileserver immer mittels Berechtigungsgruppen. In sehr seltenen Ausnahmefällen kann es jedoch notwendig sein, auf manchen Fileservern Berechtigungen direkt an Benutzerkonten zu vergeben. Diese Einstellung kann je Fileserver auf der Maske zur Bearbeitung der Fileserver-Einstellungen aktiviert werden. Standardmäßig ist diese Einstellung jedoch ausgeblendet und muss durch aktivieren dieser Einstellung eingeblendet werden.	Checkbox	✗
Vererbung - Standardwert	Legt fest, ob bei der Anlage neuer Verzeichnisse die Vererbung standardmäßig aktiviert oder deaktiviert ist.	Checkbox	✗
Vererbung - änderbar	Legt fest, ob bei der Anlage neuer Verzeichnisse die Standardeinstellung für die Vererbung geändert werden kann.	Checkbox	✗
Verzeichnis erstellen - Kommentar erforderlich	Bei der Anlage eines neuen Verzeichnisses kann ein Kommentar eingegeben werden. Diese Einstellung legt fest, ob dieser Kommentar verpflichtend ist oder nicht.	Checkbox	✗
Verzeichnis löschen - Kommentar erforderlich	Bei der Löschung eines bestehenden Verzeichnisses kann ein Kommentar eingegeben werden. Diese Einstellung legt fest, ob dieser Kommentar verpflichtend ist oder nicht.	Checkbox	✗

Verzeichnis verlängern - Tage	Legt fest um wie viele Tage das Ablaufdatum eines Verzeichnisses erhöht wird, wenn das Verzeichnis verlängert wird.	Text	✗
Verzeichnisberechtigungen bearbeiten - Kommentar anzeigen	Legt fest, ob bei der Bearbeitung von Verzeichnisberechtigungen ein Kommentar angegeben werden kann.	Checkbox	✗
Verzeichnisberechtigungen bearbeiten - Kommentar erforderlich	Legt fest, ob bei der Bearbeitung von Verzeichnisberechtigungen die Eingabe eines Kommentares verpflichtend ist. Dies setzt voraus, dass die vorhergehende Einstellung aktiv ist.	Checkbox	✗
> Genehmigungsworkflows			
Aktivieren der Prüfung der erforderlichen Personfelder bei Genehmigung per Link	Seit der Version tenfold 2022 R2 Update 2, prüft tenfold bei der Genehmigung von Personendaten-Requests mittels E-Mail-Links, ob alle erforderlich markierten Felder ausgefüllt wurden. Ist dies nicht der Fall, wird der Request nicht genehmigt, stattdessen wird der Benutzer aufgefordert bei der Genehmigung die erforderlichen Felder einzugeben. Dies war in früheren Versionen von tenfold nicht der Fall. Bei der Genehmigung über einen E-Mail-Link wurde der Request auch dann genehmigt, wenn es erforderliche Felder ohne Inhalt gab. Mit dieser Einstellung können Sie die Prüfung deaktivieren und wieder zum alten Verhalten von tenfold zurückkehren.	Checkbox	✗
Anwendungsberechtigung-Request - Übergeordneter Request	Bei der Anfrage von Berechtigungen im Zusammenhang mit einer gemeinsamen Bestellung einer Ressource entstehen zwei Requests. Der Request für die Ressource und ein weiterer Request für die Berechtigungen. Sind Genehmigungen im Spiel, kann es vorkommen, dass die Berechtigungen genehmigt werden, bevor der Ressourcen-Request fertig genehmigt oder abgearbeitet wurde. Dieser Parameter regelt, wie sich die Durchführung der Berechtigungen in diesem Fall verhält: <ul style="list-style-type: none"> • Ignorieren: Der Berechtigungs-Request wird in jedem Fall durchgeführt. • Fertig: Der Berechtigungs-Request wird nur durchgeführt, wenn der übergeordnete Ressourcen-Request fertig ist. 	Auswahl	✗

Execute EXEC 'Request.onApproved'	Diese Einstellung legt fest, ob der System-EXEC "Request.onApproved" nach jeder Genehmigung eines Genehmigungsschrittes durchgeführt wird. Sollten Sie diesen EXEC nicht verwenden, können Sie diesen Systemparameter deaktivieren um ein wenig Platz in den Log-Dateien und Durchführungszeit zu sparen.	Checkbox	
Genehmigungsworkflo w für automatische Antworten aktivieren	Mit dieser Einstellung kann für Requests zur Einrichtung einer automatischen Antwort (Exchange Abwesenheitsnachrichten) ein Genehmigungsworkflow gestartet werden. Der Genehmigungsworkflow wird normal ermittelt wie es für andere Requests zu diesem Postfach passieren würde. Ist diese Einstellung deaktiviert, wird unabhängig von den eingestellten Genehmigungsworkflows, bei Anfragen automatischer Antworten niemals ein Genehmigungsworkflow ausgelöst.	Checkbox	
Request genehmigen - Betroffene Objekte immer anzeigen	Bei der Anzeige eines Requests ist es abhängig von den Berechtigungen der angemeldeten Person, ob sich diese Details zu den Objekten (Active Directory, Microsoft 365, etc) anzeigen lassen können. Ist diese Einstellung aktiv, können sich Genehmiger, während der Genehmigung von Requests, die Details dieser Objekte immer anzeigen lassen, unabhängig von den Berechtigungen. Hinweis: Dies gilt nur während der Genehmigung des Requests. Bei der normalen Anzeige eines Requests hat diese Einstellung keine Auswirkung.	Checkbox	
Request genehmigen - Personendaten immer anzeigen	Bei der Anzeige eines Requests ist es abhängig von den Berechtigungen der angemeldeten Person, ob sich diese Details zu der Zielperson des Requests anzeigen lassen können. Ist diese Einstellung aktiv, können sich Genehmiger, während der Genehmigung von Requests, die Details dieser Personen immer anzeigen lassen, unabhängig von den Berechtigungen. Hinweis: Dies gilt nur während der Genehmigung des Requests. Bei der normalen Anzeige eines Requests hat diese Einstellung keine Auswirkung.	Checkbox	
Request genehmigen - Tab 'Offene Requests' anzeigen	Legt fest ob der Karteireiter "Offene Requests" auf der Maske zur Genehmigung von Requests angezeigt wird. Dieser Karteireiter zeigt andere offene Requests zur Zielperson des Requests an.	Checkbox	

Untergeordnete Requests bei Personenanlage - Genehmigungsmodus	<p>Im Rahmen der Neuanlage von Personen können für diese Person Ressourcen bestellt werden. Diese Einstellung regelt, wie die daraus resultierenden Requests genehmigt werden sollen.</p> <ul style="list-style-type: none"> • Automatisch genehmigen: Die Ressourcen-Requests werden, unabhängig von den Berechtigungen der anlegenden Person, automatisch genehmigt. • Mit letztem Genehmiger genehmigen: Es wird versucht soweit wie möglich mit dem letzten Genehmiger des Personenanlage-Requests jeden einzelnen Ressourcen-Request zu genehmigen. 	Auswahl	
Untergeordnete Requests bei Personenanlage - Genehmigungsumfang	<p>Im Rahmen der Neuanlage von Personen können für diese Person Ressourcen bestellt werden. Diese Einstellung legt fest, welche dieser Requests mit der Personenanlage mitgenehmigt werden sollen.</p> <ul style="list-style-type: none"> • Alle Requests: Alle untergeordneten Requests werden gemäß der Einstellung "Untergeordnete Requests bei Personenanlage - Genehmigungsmodus" genehmigt. • Alle Requests außer Anwendungsberechtigungs-Requests: Wie oben, jedoch nur für Requests welche keine Anwendungsberechtigungs-Requests sind. • Keine Requests: Keine Genehmigung findet statt. Die untergeordneten Requests müssen separat genehmigt werden. Diese Einstellung setzt den Systemparameter "Untergeordnete Requests bei Personenanlage - Genehmigungsmodus" außer Kraft. 	Auswahl	
> Jobs			
Ablaufdatum-Überprüfung - Aktiv	<p>Legt fest, ob der interne Job zur Prüfung und Entfernung abgelaufener Zuordnungen aktiv ist. Hinweis: Dieser Job wird auf der Maske zur Job-Verwaltung (Jobs(see page 443)) nicht angezeigt und läuft immer um 0:30. Achtung: Wenn dieser Job aktiv ist, darf der Job "Active Directory Group Expiry Date Check", welcher in älteren Installation eingerichtet wurde, nicht aktiv sein. Sie können besagten Job löschen, wenn Sie diesen Parameter aktivieren.</p>	Checkbox	

> Lizenz			
Pfad zur Lizenz-Datei	Legt den Pfad fest, unter welchem tenfold nach der installierten Lizenz-Datei sucht. Sollte eine Datei mit dem hier eingetragenen Namen nicht existieren, sucht tenfold im selben Verzeichnis nach Dateien mit der Endung .lic und verwendet die erste Datei (alphabetisch) welche gefunden wird.	Text	✓
Pfad zur Pubring-Datei	Legt den Pfad zur Public-Keyring-Datei fest, welche tenfold zur Verifizierung der Lizenz verwendet. Achtung: Wird diese Datei nicht gefunden, kann tenfold die Lizenz nicht verifizieren und verweigert den Start.	Text	✓
> Logging			
Archiv komprimieren	Ist diese Einstellung aktiv, werden bei der Archivierung von Log-Dateien, die archivierten Dateien komprimiert (ZIP).	Checkbox	✗
Archiv Pfad	Legt den Pfad, relativ zum Log-Datei-Pfad, auf dem tenfold-Server fest, in welchem archivierte Log-Dateien platziert werden.	Text	✗
Archiviere Log Files nach X Tagen	Legt die Anzahl in Tagen fest, nach welchen eine Log-Datei archiviert wird.	Text	✗
Lösche Log Files im Archiv	Legt fest, ob archivierte Log-Dateien nach einer gewissen Zeit im Archiv, komplett gelöscht werden sollen	Checkbox	✗
Lösche Log Files im Archiv nach X Tagen	Legt fest, nach wie vielen Tagen im Archiv, eine archivierte Log-Datei gelöscht werden soll.	Text	✗
Personen-Lifecycle-Job-Logging - Aktiv	Dieser Systemparameter steuert, ob der Job zum automatischen Übergang von Lifecycle-Phasen Log-Ausgaben tätigt oder nicht.	Checkbox	✗
REST-Connector-Logging - Aktiv	Legt fest, ob die Aufrufe von REST-APIs Detailinformationen zu den Aufrufen loggen sollen.	Checkbox	✗
Überprüfungszeitpunkt	Definiert die Uhrzeit (0-23), zu welcher die Log-Dateien archiviert werden sollen.	Text	✗
> Massenänderungen			

'Person aktualisieren' anzeigen	Steuert, ob die Option 'Person aktualisieren' im Menü Personen > Massenänderung angezeigt wird. Wird diese Option nicht angezeigt, können über die Massenänderung nur neue Personen angelegt werden.	Checkbox	✗
'Person anlegen' anzeigen	Steuert, ob die Option 'Person anlegen' im Menü Personen > Massenänderung angezeigt wird. Wird diese Option nicht angezeigt, können über die Massenänderung nur bestehende Personen aktualisiert werden. Sind beide Systemparameter deaktiviert, kann die Massenänderung nicht durchgeführt werden.	Checkbox	✗
> Microsoft 365			
Mitglieder bearbeiten - Kommentar erforderlich (Self-Service)	Legt fest, ob die Eingabe eines Kommentares zur Bearbeitung von Gruppenmitgliedern in Microsoft 365 über den Self-Service, erforderlich ist oder nicht.	Checkbox	✗
> Passwort-Portal			
Domänenauswahl anzeigen	Legt fest, ob im Passwort-Portal, die Auswahl einer Domäne möglich ist.	Checkbox	✗
Erfolgreich zurückgesetzte Passwort Anzeigen	Steuert, ob nach erfolgreicher Zurücksetzung des Passwortes mit dem Passwort-Portal, das Passwort angezeigt werden kann	Checkbox	✗
Großes Logo	Mit diesem Systemparameter kann das große Logo im Passwort-Portal angepasst werden. Verwenden Sie diesen Parameter um im Passwort-Portal ein Corporate-Design zu definieren.	Text	✗
Kleines Logo	Mit diesem Systemparameter kann das kleine Logo im Passwort-Portal angepasst werden. Verwenden Sie diesen Parameter um im Passwort-Portal ein Corporate-Design zu definieren.	Text	✗
Link zu Portal auf Login-Seite anzeigen	Steuert, ob ein Link zum Passwort-Portal auf der Anmeldemaske von tenfold angezeigt wird.	Checkbox	✗
Titel	Legt den Titel der Webseite des Passwort-Portals fest, welcher in der Titelleiste des Browsers angezeigt wird.	Text	✗
> Passwort-Reset			