



tenfold Dokumentation

tenfold 2022 R3 (22.3)

1 Inhaltsverzeichnis

1	Inhaltsverzeichnis	2
2	Installation	26
2.1	Systemvoraussetzungen	26
2.1.1	Einleitung	26
2.1.2	Systemanforderungen	26
	Applikationsserver	26
	Datenbank	27
	tenfold Agent.....	29
	Tools	29
	Datenbank	29
	Active Directory®	30
	SAP ERP®.....	30
	Andere Anwendungen	30
2.1.3	Einrichtung der Dienstkonten	30
2.1.4	Port-Freischaltungen	31
	Microsoft 365.....	32
2.2	Anlegen der Datenbank	33
2.2.1	Allgemeine Hinweise	34
2.2.2	Anlegen einer Microsoft SQL Server Datenbank.....	34
2.2.3	Anlegen einer Oracle Datenbank.....	35
2.3	Ausführung des Installationsassistenten.....	36
2.3.1	Voraussetzungen	36
2.3.2	Start	36
2.3.3	Zielordner wählen	36
2.3.4	Einspielen der Softwarelizenz	37
	Konfiguration der Datenbankverbindung	38
2.3.5	Festlegen der Web-Ports	39
2.3.6	Festlegen des SMTP-Servers	40
2.3.7	Testszenarien.....	41
2.3.8	Kopieren der Dateien und Abschluss.....	42
2.4	Installation des tenfold Agent	42
2.4.1	Aufgaben des tenfold Agent	42

2.4.2	Installation.....	43
2.4.3	Dienstanmeldung.....	45
3	Grundfunktionen	45
3.1	Systemaufbau und Begriffe.....	45
3.1.1	Organisatorischer Aufbau	45
	Personen	45
	Unternehmen.....	46
	Niederlassungen	46
	Gebäude	46
	Abteilungen	46
	Abteilungsgruppen.....	46
	Positionen.....	47
	Organisationseinheiten.....	47
	Organisationseinheitsgruppen	47
	Kostenstellen	47
	Ressourcen.....	47
	Anwendungsberechtigungen	47
	Active Directory-Gruppen.....	48
	Profile	48
	Requests.....	48
	Genehmigungsworkflow.....	48
3.2	tenfold Komponenten	49
3.2.1	tenfold Datenbank.....	49
3.2.2	tenfold Server	49
3.2.3	tenfold Agents.....	50
3.3	Self-Service-Oberfläche	51
3.3.1	Passwortänderung.....	52
3.3.2	Ressourcenanforderung	52
	Allgemeines.....	52
	Ressourcenauswahl.....	53
	Festlegung von Optionen und Berechtigungen.....	54
	Bestehende Zuordnung bearbeiten	55
	Bestehende Zuordnung löschen	55
	Spezialkategorie Fileserver	56

Spezialkategorie Active Directory-Gruppen.....	57
Spezialkategorie Profile.....	58
Ressourcensuche	60
3.3.3 Person anlegen und Personendatenänderung.....	60
3.3.4 Meine Requests	61
Filter	61
Anzeige und Aktionen	61
3.3.5 Dateneigentümerbereich	62
3.3.6 Genehmigungsworkflows.....	63
4 Personenverwaltung	63
4.1 Personen	63
4.1.1 Allgemeines.....	63
4.1.2 Personenarten.....	63
4.1.3 Personen anlegen	64
Überprüfung von existierenden Personen	64
Benutzername	65
Neue Person anlegen.....	66
Person nach Profil anlegen	66
Person mit zweiter Person als Vorlage anlegen	66
Allgemeine Funktionen	67
Stammdateneingabe	67
Ressourcen.....	69
Lifecycle	71
Dokumente	74
Speichern.....	75
4.1.4 Personen bearbeiten.....	75
4.1.5 Personen sperren.....	76
4.1.6 Personen entsperren	77
4.1.7 Personen löschen	78
4.1.8 Berichte.....	79
Neuen Bericht erzeugen	79
4.2 Personenarten.....	81
4.2.1 Allgemeines.....	81
4.2.2 Anzeige.....	82
4.2.3 Anlegen oder Bearbeiten	82

	Allgemein.....	82
	Genehmigungsworkflows.....	90
	Passwort-Reset.....	91
	Parameter.....	92
	Provisioning.....	93
	Felder.....	93
4.2.4	Löschen.....	103
4.3	Verknüpfte Personen.....	103
4.3.1	Einstellungen.....	103
4.3.2	Personen verknüpfen.....	107
	Verknüpfte Person anlegen.....	107
	Personen manuell verknüpfen.....	108
	Verknüpfungsassistent.....	109
	Verknüpfung aufheben.....	111
4.3.3	Datenabgleich.....	112
4.4	Titel.....	114
4.5	Positionen.....	115
4.6	Personenlisten.....	116
4.6.1	Mitglieder verwalten.....	116
4.7	Request-Begründungen.....	117
4.7.1	Allgemeines.....	117
4.7.2	Konfiguration.....	117
	Einrichtung der Begründungen.....	117
	Konfiguration der Personenarten.....	119
4.7.3	Nutzung.....	120
4.8	Datenkorrektur.....	120
4.8.1	Hintergrund.....	120
4.8.2	Verwendung.....	120
	Personenauswahl.....	121
	Anzeige des Vergleichs.....	121
	Auswahl der Änderungen.....	122
	Durchführung.....	122
4.8.3	Reporting.....	123
5	Ressourcen.....	125

5.1	Ressourcenverwaltung	125
5.1.1	Allgemeines.....	125
5.1.2	Anzeige.....	125
5.1.3	Bearbeitung	126
	Allgemein.....	127
	Self Service.....	131
	Verfügbarkeit.....	135
	Genehmigungsworkflow.....	136
	Parameter	138
	Optionen	138
	Informationsfelder	139
	Dateneigentümer	139
	Kontexte	140
	Berechtigungen	141
	Provisioning.....	144
	Erweiterte Einstellungen.....	146
5.1.4	Löschen	149
5.1.5	Kopieren	149
5.2	Ressourcenkategorien.....	149
5.2.1	Allgemein.....	149
5.2.2	Verwaltung	150
5.3	Optionen für Ressourcen.....	151
5.3.1	Allgemein.....	151
5.3.2	Anlage und Bearbeitung	152
	Allgemein.....	152
	Datentyp Selection.....	153
	Datentyp String.....	153
5.3.3	Löschen	154
5.4	Servicelevels.....	154
5.4.1	Allgemein.....	154
5.4.2	Verwaltung	154
5.5	Lizenzpools	156
5.5.1	Allgemein.....	156
5.5.2	Verwaltung	156

	Lizenzpool	157
	Verträge	158
	Benachrichtigungen	159
	Ressourcen	160
5.5.3	Analyse	160
5.6	Ressourcenzuordnungen	161
5.6.1	Allgemein	161
5.6.2	Zuordnungen anzeigen	162
5.6.3	Berechtigungen anzeigen	162
5.7	Dateneigentümer	163
5.7.1	Übersicht	163
5.7.2	Nachfolger	165
6	Profile	168
6.1	Verwaltung	168
6.1.1	Allgemeines	168
6.1.2	Anzeige	168
6.1.3	Neuanlage und Bearbeitung	169
	Allgemein	169
	Self-Service	171
	Ressourcen	173
	Verfügbarkeit	175
	Genehmigungsworkflows	176
	Automatische Zuordnung	178
6.1.4	Export von Profilen	179
6.2	Zuordnung	181
6.2.1	Bedienung	182
6.2.2	Anzeige	182
6.2.3	Typ ändern	183
6.3	Zuordnungen: Detailansicht	184
6.4	Abweichungen	184
6.4.1	Allgemeines	184
6.4.2	Bedienung	184
	Anzeige	184
	Optionen	185

6.4.3	Weitere Schritte.....	185
6.5	Profilassistent	185
6.5.1	Anwendungsbereich	185
6.5.2	Bedienung.....	186
	Auswahl und Anzeige	186
	Zusatzfunktionen	188
6.5.3	Profilimport	189
6.6	Abgleich.....	192
6.6.1	Einleitung.....	192
6.6.2	Abgleich aus dem Profil	192
6.6.3	Abgleich aus der Person.....	192
6.7	Automatischer Abgleich	192
7	Verwaltung der Microsoft-Systeme	196
7.1	Konfiguration.....	196
7.1.1	Einrichten einer Windows Domain	196
	Einführung	196
	Anlegen der Domain	196
7.1.2	Einrichten des tenfold Agent.....	199
	Allgemeine Informationen	199
	Agent installieren	199
	Konfiguration des Agent.....	200
	Agent in tenfold einbinden	204
7.1.3	WMI-Remotezugriff.....	204
	Vorraussetzungen.....	204
	Vorgehensweise.....	204
7.1.4	Berechtigungsstufen	205
	Allgemein.....	205
	Anzeige.....	206
	Bearbeitung	206
7.1.5	Fileserver-Berechtigungsgruppen	207
	Allgemeines.....	207
	Anlegen einer neuen Konfiguration	207
	Konfiguration in einer Domäne verwenden	210
	Bearbeiten einer Konfiguration	211

	Löschen einer Konfiguration	212
7.1.6	Exchange-Berechtigungsgruppen	212
	Allgemeines	212
	Anlegen einer neuen Konfiguration	212
	Bearbeiten einer Konfiguration	214
	Löschen einer Konfiguration	214
	Anzeige bestehender Berechtigungsgruppen	214
	Berechtigungsgruppen importieren	215
7.1.7	SharePoint-Berechtigungsgruppen	217
	Allgemeines	217
	Gruppeneinstellungen verwalten	217
	Anzeige bestehender Berechtigungsgruppen	221
	Berechtigungsgruppen importieren	222
7.1.8	Einrichtung der Fileserver	223
	Auswahl der Domäne	223
	Einstellungen für die Domäne	224
	Einstellungen für einen Fileserver	225
	Scan der Fileserver	233
7.1.9	Einrichtung der Exchange Server	233
	Allgemeines	233
	Einrichtung des Exchange-Servers	234
	Scan der Exchange-Server	238
7.1.10	Einrichtung der SharePoint-Server	238
7.1.11	Active Directory Kategorien	242
	Allgemein	242
	Verwaltung	242
7.1.12	Einrichtung von Microsoft 365 Mandanten	243
	Microsoft 365 Mandant vorbereiten	243
	Vorbereitung des Agents	251
	Einrichtung des Mandanten in tenfold	252
	SharePoint	259
	Teams	261
	OneDrive	263
	Datenabgleich	263
	Microsoft 365 User Lifecycle Plugin	263

7.2	Verwaltung der Active Directory Gruppen	265
7.2.1	Funktionalität	265
7.2.2	Einstiegsmaske	266
	Neue Gruppe anlegen	266
7.2.3	Gruppeneinstellungen bearbeiten	267
7.2.4	Mitgliedschaften bearbeiten / Dateneigentümer festlegen	268
7.2.5	Gruppe löschen	269
7.2.6	Gruppe umbenennen	269
7.2.7	Pathfinder	269
7.3	Verwaltung der Fileserver-Berechtigungen	269
7.3.1	Allgemeines	269
	Sichten	270
	Aufbau	270
7.3.2	Berechtigungen anzeigen	271
	Verzeichnisbaum	271
	Anzeigebereich - Berechtigungsbaum	272
	Anzeigebereich - Berechtigungspfade	273
7.3.3	Historische Ansicht	274
7.3.4	Erweiterte Eigenschaften anzeigen	275
7.3.5	Verlauf anzeigen	276
7.3.6	Berechtigungen bearbeiten	276
	Berechtigungen anzeigen	277
	Detailinformationen anzeigen	278
	Neue Berechtigung setzen	279
	Berechtigungen befristen	280
	Berechtigung löschen	280
	Änderungen speichern	280
7.3.7	Berechtigungsbericht	281
7.3.8	Verfügbarkeit festlegen	284
7.3.9	Weitere Aktionen	287
	Verzeichnis anlegen	287
	Verzeichnis umbenennen	288
	Verzeichnis löschen	288
	Vererbung ändern	289
	Dateneigentümer festlegen	289

Einstellungen.....	292
Ablaufdatum setzen	292
Aktualisieren.....	293
7.3.10 Microsoft DFS	293
7.4 Verwaltung der Exchange-Berechtigungen	294
7.4.1 Allgemeines.....	294
Aufbau	294
7.4.2 Berechtigungen Anzeigen	295
Objektbaum	295
Anzeige - Berechtigungsbaum	296
Anzeigebereich - Berechtigungspfade.....	298
7.4.3 Postfach- und Ordnerberechtigungen bearbeiten.....	299
Berechtigungen anzeigen.....	300
Detailinformationen anzeigen.....	300
Neue Berechtigung setzen	301
Berechtigungen befristen	302
Berechtigung löschen	302
Änderungen speichern.....	303
7.4.4 Weitere Aktionen.....	303
Automatisch Antworten.....	303
Stellvertreter	305
Aktualisieren.....	307
Dateneigentümer	308
Einstellungen.....	308
7.5 Verwaltung der SharePoint-Berechtigungen	309
7.5.1 Allgemeines.....	309
7.5.2 Berechtigungen anzeigen.....	310
7.5.3 Berechtigungen bearbeiten	312
Vergabe neuer Berechtigungen.....	313
Entfernen vorhandener Berechtigungen.....	313
Ablaufdatum von Berechtigungen ändern.....	313
Vererbung ändern	314
7.5.4 Einstellungen bearbeiten	318
Allgemeine Einstellungen	318
7.5.5 Dateneigentümer	320

7.5.6	Self-Service.....	322
7.6	Verwaltung der Microsoft 365 Lizenzen	324
7.6.1	Vergabe von Lizenzen.....	325
7.6.2	Entzug von Lizenzen	327
7.6.3	Dateneigentümer bearbeiten.....	329
7.7	Verwaltung der Microsoft 365 Gruppen	331
7.7.1	Bereich Zuordnungen (Zentraler Bereich)	331
7.7.2	Bereich Office 365-Objekte (Linker Bereich)	332
	Hinzufügen von Mitgliedern und Besitzern	333
	Hinzufügen von Dateneigentümern	334
7.7.3	Bereich Details (Rechter Bereich)	335
7.8	Microsoft Teams.....	337
7.8.1	Übersicht	338
7.8.2	Dateneigentümer	341
7.8.3	Microsoft 365 Teams-Vorlagen	344
	Teams mittels Vorlage anfordern	347
8	Funktionen für Suche und Reporting	348
8.1	Active Directory Pathfinder	348
8.2	Schnellsuche	350
8.2.1	Sucheinstellungen.....	350
8.2.2	Suche ausführen	350
8.2.3	Suchergebnis.....	351
8.2.4	Weitere Aktionen.....	351
8.3	Requests.....	352
8.3.1	Definition	352
8.3.2	Liste der Requests	354
	Allgemeines.....	354
	Filter	354
	Ergebnis.....	355
8.3.3	Requests anzeigen.....	356
	Karteireiter Allgemeines	357
8.4	Personensuche	357
8.4.1	Personen suchen (Standardsuche)	358
8.4.2	Personen suchen (Feldregelsuche)	359

8.4.3	Angezeigte Felder	360
8.4.4	Excel-Export.....	361
8.4.5	Aktionen.....	362
8.5	Dashboard	362
9	Organisationsstruktur	366
9.1	Abteilungen	366
9.1.1	Abteilungen	366
9.1.2	Abteilungsverantwortliche	368
9.1.3	Abteilungsgruppen.....	368
9.1.4	Abteilungshierarchie.....	369
9.2	Kostenstellen	369
9.3	Organisationseinheiten.....	369
9.3.1	Organisationseinheiten.....	369
9.3.2	Organisationseinheitsgruppen	371
9.4	Stellvertretungen	372
9.4.1	Allgemeines.....	372
9.4.2	Stellvertreter einstellen.....	372
9.4.3	Stellvertreter für andere.....	373
9.4.4	Organisationsabhängige Berechtigungen	375
9.4.5	Anzeige.....	375
9.4.6	Vererbung	376
9.5	Unternehmen & Niederlassungen	377
9.5.1	Unternehmen.....	377
9.5.2	Niederlassungen	378
9.5.3	Gebäude	380
10	Workflows.....	380
10.1	Genehmigungsworkflows.....	380
10.1.1	Zweck	380
10.1.2	Auswahl des Workflows	380
10.1.3	Rollen innerhalb eines Workflow.....	381
10.1.4	Requeststatus	382
10.1.5	Verwendung ermitteln	382
10.2	BPMN-Genemigungsworkflows.....	383
10.2.1	Anlegen eines BPMN-Genemigungsworkflows	386

Genehmigungsschritt hinzufügen.....	389
Interaktive Aktivität hinzufügen	392
Vordefinierte Aktivität hinzufügen	393
EXEC hinzufügen.....	393
Verzweigungen hinzufügen.....	394
Parallele Genehmigungsworkflows hinzufügen	395
Zeitliche Beschränkungen hinzufügen	397
Nachrichtenempfang hinzufügen	399
Automatische Genehmigung unterbrechen	400
10.2.2 Workflows bearbeiten und löschen	400
10.3 Kontexte (Workflow)	401
10.3.1 Hintergrund	401
10.3.2 Verwaltung	401
10.3.3 Einstellungen (Workflow)	403
10.3.4 Nutzung	403
10.4 Lifecycle	404
10.4.1 Grundlagen	404
10.4.2 Konfiguration.....	405
Allgemein.....	405
Self-Service.....	406
Feldregeln.....	407
Aktionen.....	407
Automatischer Phasenwechsel	411
Genehmigungsworkflow.....	414
10.4.3 Änderungen	414
Über "Person bearbeiten"	415
Über Self-Service	416
11 Rezertifizierung	417
11.1 Richtlinien	418
11.1.1 Anlage neuer Richtlinien	419
11.1.2 Weitere Aktionen.....	429
11.2 Rezertifizierungsprozesse.....	430
11.2.1 Übersicht der Prozesse	430
11.2.2 Rezertifizierungen durchführen.....	435

12	Einstellungen	437
12.1	Application Server	437
12.1.1	RAM-Einstellungen	437
	Bedeutung	437
	Ändern der Einstellung	437
	Überprüfen der Einstellung	437
	Troubleshooting	438
12.1.2	Datenbankverbindung	438
	Änderungen	438
	Anpassung der Verbindung	439
	Troubleshooting	440
	Art und Anzahl der Verbindungen	441
12.1.3	Einrichten von Single Sign On	441
	Aktivierung bei einer neuen Installation	441
	Aktualisierung der Einstellungen bei bestehenden Installationen	441
12.2	Wartungsmodus	442
12.3	Jobs	443
12.3.1	Allgemeines	443
12.3.2	Verwaltung	444
	Spezielle Jobs	444
	Liste der Jobs	444
	Job-Einstellungen bearbeiten	445
	Job löschen	446
	Job ausführen	446
	Ausführung abbrechen	446
12.3.3	Historie	447
12.4	Benachrichtigungen	448
12.4.1	Kanäle	448
12.4.2	Verwaltung	450
	Allgemeine Einstellungen	452
12.4.3	Übersicht	455
12.5	Berechtigungen	457
12.5.1	Berechtigungen	457
12.5.2	Rollen	458

12.5.3	Verwaltung der Berechtigungen.....	458
12.5.4	Rollen	459
	Einzelberechtigungen / Karteireiter "Rolle"	460
	Personenarten.....	461
	Domänen	461
	Microsoft 365-Mandanten.....	462
	Fileserver	463
	Exchange-Server	464
	SharePoint	464
	Provisioning.....	464
	Verzeichnisvorlagen	464
12.5.5	Rollenzuordnung	465
12.5.6	Auswertung	467
12.5.7	Vordefinierte Berechtigungen	468
12.6	Zwei-Faktor-Authentifizierung (2FA)	480
12.6.1	Zweck	480
12.6.2	Funktionsweise	481
12.6.3	Konfiguration.....	481
12.6.4	Benutzer festlegen.....	481
12.6.5	Benutzerkonfiguration	482
12.6.6	Token-Verwaltung	483
12.7	Systemparameter	484
12.7.1	Allgemeines.....	485
	Standardparameter.....	485
	Benutzerdefinierte Parameter	486
12.7.2	Verwaltung von Systemparametern	486
12.7.3	Liste der Standardparameter	486
12.8	Berichtvorlagen	520
12.9	Sessionverwaltung.....	521
12.9.1	Aktuelle Sessions.....	521
12.9.2	Session ändern.....	523
12.10	Zertifikatsverwaltung.....	523
12.11	Softwarelizenz.....	524
12.11.1	Allgemeines.....	524

12.11.2 Installation einer neuen Lizenz	525
12.11.3 Lizenzeinstellungen	525
Ausnahmen festlegen.....	527
Auswertung	530
12.11.4 Mögliche Probleme.....	531
Keine Lizenzdatei gefunden	531
Lizenz abgelaufen.....	531
12.12 SMTP-Server.....	532
12.12.1 Allgemeine Einstellungen	533
12.12.2 SMTP-Server Einstellungen.....	533
12.12.3 Testmail senden.....	535
12.13 Historie gesendeter E-Mails	536
12.13.1 Allgemeine Informationen	536
12.13.2 Anzeige gesendeter E-Mails.....	538
12.13.3 Erneutes Senden von E-Mails.....	539
12.14 Passwortrichtlinien	539
12.14.1 Erstellen und Bearbeiten von Passwortrichtlinien	540
12.14.2 Passwortrichtlinien anwenden.....	543
12.15 Verifizierungsrichtlinien.....	543
12.15.1 Allgemeines.....	544
12.15.2 Verwaltung von Verifizierungsrichtlinien.....	544
Allgemeine Einstellungen	545
PIN-Einstellungen.....	546
Sicherheitsfragen.....	550
Active Directory-Passwort.....	551
Einmalpasswort	551
13 Provisioning.....	552
13.1 Zugangsdaten	552
13.1.1 Allgemeines.....	552
13.1.2 Verwaltung	552
13.1.3 Anlage und Bearbeitung	554
Bedeutung von Verbindung 1/2	554
13.1.4 Active Directory	555
13.2 Feldmappings.....	556

13.2.1	Allgemeines.....	556
13.2.2	Nutzung in Plugins.....	556
13.2.3	Verwaltung	557
13.2.4	Anlage und Bearbeitung	557
	Feld hinzufügen oder bearbeiten	558
	Feld entfernen	560
	Import und bidirektionale Verarbeitung.....	560
	Schlüsselfelder.....	560
13.2.5	Kopieren	562
13.2.6	Löschen	562
13.2.7	Weiterführende Hinweise	562
13.3	Feldregeln	562
13.3.1	Allgemein.....	562
13.3.2	Verwaltung von Feldregeln.....	563
13.3.3	Anlage und Bearbeitung	564
	Kopfdaten	564
	Bedingungen	564
13.3.4	Vereinfachte Anlage	572
13.3.5	Duplikate.....	572
13.4	Benutzerkonto-Auswahl	573
13.4.1	Neue Regel erstellen	573
13.4.2	Vorhandene Regel bearbeiten od. löschen.....	576
13.4.3	Auswertung von Regeln.....	577
13.5	Bedingungen	578
13.5.1	Einzelbeschreibung.....	579
13.5.2	Personenkreise	582
13.5.3	Verwendung	583
13.5.4	Anwendungsbeispiel.....	584
13.6	Regeln für Benutzernamen	585
13.6.1	Allgemeines.....	585
13.6.2	Verwaltung	585
13.6.3	Verwaltung der Regeln.....	586
	Regeleinstellungen.....	586
13.6.4	Anwendungsbereich der Regeln	591
	Zweck	591

Verwaltung	592
13.7 User Principal Names	593
13.7.1 Allgemeines.....	593
13.7.2 Regeln anlegen oder bearbeiten	594
13.7.3 Verwendung der Regeln festlegen.....	598
13.7.4 Feldmapping oder Regel.....	600
13.8 E-Mail-Adressen	600
13.8.1 Regeln anlegen oder bearbeiten	601
13.8.2 Regelwerk aktivieren.....	601
13.9 Generierte Werte	603
13.9.1 Hintergrund	603
13.9.2 Konfiguration.....	603
Basiselemente.....	603
Trigger	604
Modus.....	604
Action.....	604
13.9.3 Nutzung	605
In Personenfeldern.....	605
In Feldmappings	606
13.9.4 Abgleich.....	606
13.10 Datentypen	608
13.10.1 Allgemein.....	608
13.10.2 Verfügbare Datentypen.....	608
13.10.3 Benutzerdefinierte Auswahl	609
13.11 Datenstrukturen	610
13.11.1 Request.....	610
RequestStatus.....	612
RequestType	613
RequestMode	613
13.11.2 Person.....	614
13.11.3 PersonMasterdata	614
13.11.4 Department.....	617
13.11.5 Service	618
13.12 tenfold Agenten.....	619

13.12.1 Registrierung neuer Agents.....	620
13.12.2 Agenten aktualisieren.....	623
13.12.3 Individuelle Zertifikate erstellen.....	624
13.12.4 Web Service Endpoints verwalten.....	627
13.13 Aktivitäten.....	628
13.13.1 Interaktive Aktivitäten.....	628
Definition interaktiver Aktivitäten.....	629
Interaktive Aktivitäten einbinden.....	637
Interaktive Aktivitäten abschließen.....	638
13.13.2 Vordefinierte Aktivitäten.....	643
Vordefinierte Aktivitäten erstellen.....	645
Einsetzen vordefinierter Aktivitäten.....	646
13.13.3 Aktivitätsliste.....	647
13.14 Erzeugung von Passwörtern.....	648
13.14.1 Herkömmliche Passwortvergabe.....	648
13.14.2 Passwörterzeugung durch tenfold.....	649
Einstellungen zur Erzeugung des Passwortes.....	652
Empfängereinstellungen.....	653
13.14.3 One-Time-Secrets.....	658
14 Plugins.....	660
14.1 Allgemeine Informationen zu Plugins.....	660
14.1.1 Verwaltung der Plugins.....	661
14.1.2 Installation von Plugins.....	662
14.1.3 Konfiguration von Plugins.....	663
Globale Einstellungen.....	664
Einstellungen für Ressourcen.....	664
Einstellungen für Personenarten.....	664
14.1.4 Deinstallation von Plugins.....	665
14.1.5 Häufige Einstellungen.....	665
Code Snippet.....	665
Feldregeln.....	665
Feldmapping.....	665
14.2 Active Directory User Lifecycle.....	665
14.2.1 Übersicht über die Einstellungen.....	666

14.2.2	Organisationseinheiten.....	667
	Verhalten	667
	Einstellungen.....	668
	Beispiel	668
14.2.3	Benutzer anlegen	669
	Benutzeranlage	669
14.2.4	Benutzer ändern.....	672
	Benutzer verschieben	672
14.2.5	Benutzer sperren.....	672
	Gruppenmanagement.....	673
	Verschieben.....	674
14.2.6	Benutzer löschen	674
	Aktion in Active Directory	674
	Entscheidungstabelle	675
14.2.7	Automatische Aktionen	675
	Austrittsdatum	675
	Inaktive Benutzer	676
14.2.8	Passwort-Reset	678
14.2.9	Personenart.....	679
	Entscheidungstabelle	680
	Standard-Personenart.....	681
	Beispiel	681
14.2.10	Feldmapping.....	682
	Tabelle Feldmapping - Decision Table	683
	Bereich Einstellungen	684
14.2.11	Domänen	687
14.3	Active Directory Gruppenzuweisung.....	688
14.3.1	Globale Konfiguration	689
	Import	689
14.3.2	Provisionierungskonfiguration	690
14.3.3	Synchronisierung	692
14.4	Exchange Mailbox Lifecycle.....	692
14.4.1	Lebenszyklus.....	692
14.4.2	Allgemeine Einstellungen	693
	Karteireiter "Einstellungen"	695

Karteireiter "Mailbox-Datenbanken"	699
Karteireiter "Mailbox bearbeiten"	700
Karteireiter "Mailbox löschen"	701
14.4.3 Abgleich und Simulation.....	702
14.5 Basisordner	703
14.5.1 Konfigurationsübersicht	704
14.5.2 Allgemein.....	704
14.5.3 Benutzer ändern	705
14.5.4 Ressourcen.....	705
14.6 E-Mail-Benachrichtigung.....	706
14.6.1 Konfigurationsübersicht	706
14.6.2 Allgemein.....	707
Absender	707
Betreff überschreiben	707
Benachrichtigung bei fehlgeschlagenem Request	707
Benachrichtigung bei fehlgeschlagenem Job.....	708
14.6.3 Personendaten (und folgende Karteireiter).....	708
14.6.4 Globale Ereignisse	709
14.7 Import Plugin	710
14.7.1 Konfigurationsübersicht	710
14.7.2 Allgemein.....	712
Quelle "CSV-Datei"	712
Quelle "Code Snippet"	713
14.7.3 Feldmapping.....	713
Personen-identifizierendes Feld	714
Objekte.....	715
14.7.4 Aktionen.....	716
Personen-Aktionen.....	716
Personenkreis	717
Requests.....	717
Warnung	720
14.7.5 Erweiterte Einstellungen	721
14.7.6 Simulation	722
14.8 SAP User Lifecycle.....	722
14.8.1 Konfiguration.....	723

14.8.2	Zugangsdaten	725
14.8.3	Ressource.....	726
14.8.4	Synchronisierung	728
14.9	Office 365 User Lifecycle	728
14.9.1	Konfiguration.....	728
14.9.2	Ressource.....	730
	Anlage der Ressource.....	730
	Einstellen der Lizenztypen.....	730
14.9.3	Sync-Job.....	731
14.10	Generic Connector	731
14.10.1	Plugin-Einstellungen	732
	Neues System anlegen.....	732
	Systeme bearbeiten/löschen	737
	Simulation	737
	API-Dokumentation.....	738
	Beispiele	739
14.10.2	API-Dokumentation.....	740
	Prozesse.....	741
	Endpoints.....	747
	Datenmodell	757
14.10.3	Implementierung eines APIs	772
	Schnittstellenbeschreibung herunterladen	772
	Stub herunterladen	773
	Erklärung des Stubs.....	774
	Vom Stub zum API: Tutorial 1	778
	Beispielanwendung: Sample 01	791
14.11	macmon.....	799
14.11.1	Verwendung	799
14.11.2	Plugin-Konfiguration	799
	Allgemeine Einstellungen	800
	Simulation	801
	Zugangsdaten	802
	Datenabgleich	803
14.12	Microsoft 365 User Lifecycle	803
14.12.1	Allgemeines.....	803

14.12.2 Globale Einstellungen	803
Benutzer anlegen	805
Benutzer ändern	806
Personensynchronisation	807
Personenzuordnung	813
Simulation	817
Ressourcen	818
15 Sicherheit und Datenschutz	821
15.1 Datenschutzhinweise	821
15.1.1 Zweck der Anwendung	821
15.1.2 Arten der verarbeiteten Daten	821
Benutzerstammdaten	821
Berechtigungsdaten	822
Antragsdaten	822
Systemeinstellungen	822
15.1.3 Verfahren zur Datenverarbeitung	822
15.1.4 Zugriffskontrollen	822
15.2 Datenschutzrichtlinie	822
15.2.1 Richtlinie verwalten	823
15.2.2 Manuelle Anonymisierung	825
15.2.3 Welche Daten werden anonymisiert?	826
15.3 Hinweise zu Betroffenenrechten laut DSGVO	828
15.3.1 Grundsätzliches	828
15.3.2 Recht auf Auskunft (Art. 15 DSGVO)	828
15.3.3 Recht auf Berichtigung (Art. 16 DSGVO)	828
15.3.4 Recht auf Löschung (Art. 17 DSGVO)	828
15.3.5 Recht auf Datenübertragbarkeit (Art. 20 DSGVO)	828
15.3.6 Recht auf Widerspruch (Art. 21 DSGVO)	829
15.4 Technische Sicherheitsinformationen	829
15.4.1 Allgemeine Hinweise	829
15.4.2 Datenbanksicherheit	829
Zugang zur Datenbank	829
Passworte für Fremdsysteme	830
15.4.3 Application Server	830

Verzeichnisberechtigungen.....	830
Hinweise für Dienstkonten	830
15.4.4 Netzwerksicherheit	830
Verbindung über das Web-Frontend	830
Verbindung zum Active Directory	831
Verbindungen zum tenfold Agent	831
Andere Verbindungen	831
15.5 Richtlinie zur Behebung von Sicherheits-Bugs.....	831
15.5.1 Einstufung und Behebung von Schwachstellen	831
15.6 Security Dashboard.....	832
15.6.1 Dashboard Übersicht	832
15.7 Integration von Antivirus Software	834
15.7.1 Einstellungen.....	834
15.7.2 Prüfung von Dateien	836

2 Installation

2.1 Systemvoraussetzungen

2.1.1 Einleitung

Dieser Artikel beschreibt die grundlegenden Schritte, die vor einer Installation von tenfold durchzuführen sind. Für Trial-Installationen beachten Sie bitte zusätzlich die entsprechenden Hinweise.

Fernwartung

Bitte beachten Sie, dass für die Fernwartung **ausschließlich** das Tool "TeamViewer" in der jeweils aktuellen Version zum Einsatz kommt. Dieses Werkzeug **muss nicht installiert werden**, sondern kann für die jeweilige Session ad-hoc ausgeführt werden.

Zum Starten, navigieren Sie im Browser zu <https://www.teamviewer.com/>¹ und wählen die Option "An Fernsteuerung teilnehmen"

vor Ort

Bei Leistungen vor Ort muss ein Endgerät zur Verfügung gestellt werden, mit welchem der Zugriff auf das interne Netzwerk und die jeweils benötigten Ressourcen (Server, Datenbanken, Applikationen) möglich ist.

2.1.2 Systemanforderungen

Um tenfold in Ihrer Umgebung betreiben zu können, sind systemseitig einige Anforderungen an Hard- und Software zu erfüllen. Zusätzlich kann es noch spezifische Anforderungen bei der Integration von anderen Softwareprodukten geben, welche hier nicht angeführt werden.

Applikationsserver

Für den Betrieb des tenfold Anwendungsdienstes ist ein Server erforderlich. Es werden sowohl physische als auch virtuelle Server unterstützt.

Es gelten dabei folgende Hardware-Voraussetzungen:

Mindestanforderungen	tenfold Agent auf eigenem Server	tenfold Agent auf gleichem Server
Arbeitsspeicher	8 GB	16 GB
Festplattenspeicher (verfügbar für tenfold)	10 GB	20 GB
LAN-Anbindung zum Fileserver / Exchange Server / SharePoint Server	Gbit	Gbit

Hinweis zu anderen Anwendungen

¹ <https://www.teamviewer.com/de/>

Aus Sicherheitsgründen dürfen auf dem Applikationsserver, neben tenfold, keine anderen Anwendungen betrieben werden. Die Installation von tenfold auf einem Active Directory® Domain Controller wird nicht unterstützt.

Folgende Betriebssysteme werden für den Betrieb des tenfold Anwendungsdienstes unterstützt:

- Microsoft Windows Server 2012®
- Microsoft Windows Server 2012 R2®
- Microsoft Windows Server 2016®
- Microsoft Windows Server 2019®
- Microsoft Windows Server 2022®

Hinweis zu Java® (Java Development Kit - JDK)

Für den Betrieb des Applikationsservers muss das Java® Runtime Environment installiert sein. Seit tenfold 2018 Update 2 wird das Java Runtime Environment automatisch durch den Installer installiert und bei Updates automatisch auf die richtige Version aktualisiert. Es darf darüber hinaus auf dem System, aus Kompatibilitätsgründen, keine andere JDK- oder JRE-Version installiert werden. tenfold nutzt die Implementierung "Amazon Corretto", um den Lizenz einschränkungen des Oracle® JDK/JRE zu entgehen.

Achtung: Portfreischaltung tenfold Marketplace

Damit tenfold eingerichtet und sicher betrieben werden kann, ist es unbedingt erforderlich, dass die genutzten Plugins jederzeit aktualisiert werden können. Diese Aktualisierung erfolgt über eine HTTPS-Verbindung aus dem Internet. Es ist daher erforderlich, dass der tenfold Applikationsserver eine HTTPS-Verbindung zu **marketplace.tenfold-security.com** aufbauen kann. Dazu ist gegebenenfalls eine Ausnahme in der Firewall einzurichten. Wenn Sie diese Verbindung nicht freischalten, dann müssen Sie manuell dafür sorgen, dass die Plugins regelmäßig aktualisiert werden.

Datenbank

Zur Speicherung der Einstellungen und Benutzer- und Berechtigungsdaten wird eine Datenbank benötigt. Die Datenbank muss sich nicht auf demselben System wie der Anwendungsdienst befinden. Für tenfold ist es ausreichend, wenn innerhalb einer bestehenden Datenbankinstanz (eines Datenbankservers) eine neue Datenbank (neuer Benutzer bzw. Schema) eingerichtet wird.

Folgende Datenbanksysteme werden von tenfold unterstützt:

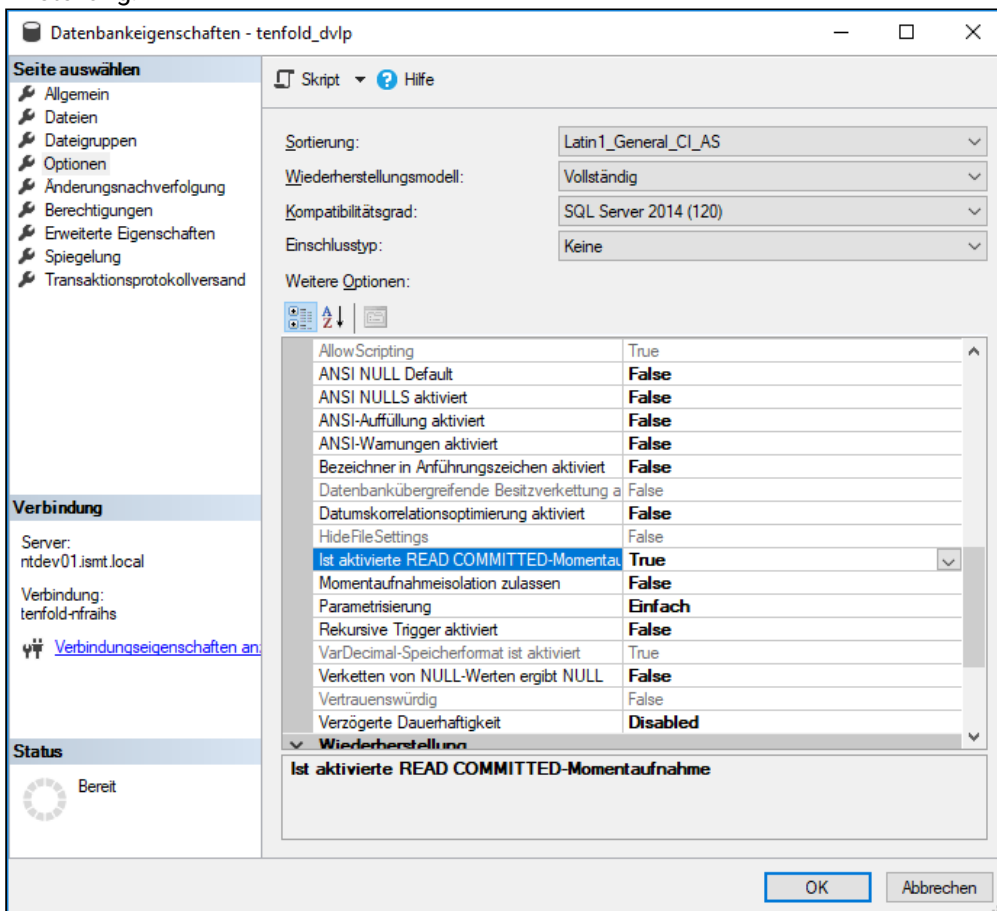
- Microsoft SQL Server 2012® Service Pack 4
- Microsoft SQL Server 2014® Service Pack 3
- Microsoft SQL Server 2016® Service Pack 2
- Microsoft SQL Server 2017®
- Microsoft SQL Server 2019®
- Oracle® Database 12.1
- Oracle® Database 12.2
- Oracle® Database 18c
- Oracle® Database 19c

Hinweise zu Microsoft SQL Server

Die Express Edition von Microsoft SQL Server® wird von tenfold unterstützt. Aufgrund der Performance- und Größenbeschränkungen sollten Sie jedoch vor Verwendung Ihren tenfold Betreuer kontaktieren, um mögliche Probleme im Vorhinein auszuschließen.

Achtung: Der Authentifizierungstyp "Windows-Authentifizierung" wird bei Microsoft SQL Server® bei Always-On-Clustern nicht unterstützt.

Bitte beachten Sie, dass bei Microsoft SQL Server für die Datenbank die Einstellung "Ist aktivierte READ COMMITTED-Momentaufnahme" unbedingt auf den Wert "True" gesetzt werden muss, da tenfold sonst in bestimmten Situationen nicht ordnungsgemäß funktioniert. Der nachfolgende Screenshot zeigt diese Einstellung:



Hinweise zu Oracle

Die Express Edition von Oracle® wird von tenfold unterstützt. Aufgrund der Performance- und Größenbeschränkungen sollten Sie jedoch vor Verwendung Ihren tenfold Betreuer kontaktieren, um mögliche Probleme im Vorhinein auszuschließen. **Achtung:** Es ist der Zeichensatz "UTF8" zwingend erforderlich. Andere Zeichensätze werden nicht unterstützt.

Nicht unterstützte Datenbanken

Die Installations- und Update-Assistenten werden Sie darauf hinweisen, wenn Ihre Datenbank nicht (mehr) unterstützt wird.

tenfold Agent

Der tenfold Agent stellt Funktionen für das Auslesen und Setzen von Berechtigungen auf NTFS File Servern, Microsoft Exchange® und Microsoft SharePoint® zur Verfügung. Bei Einbindung von File Servern wird, je Standort, eine Agent-Instanz benötigt (für Standorte, bei denen die File Server über schnelle Netzwerkverbindungen zum tenfold Applikationsserver verfügen (zumindest Gigabit), ist keine separate Instanz erforderlich). Bei Einbindung von Microsoft Exchange® wird, pro Exchange-Organisation, und bei Einbindung von Microsoft SharePoint® pro SharePoint-Farm, je eine Agent-Instanz benötigt.

Für die Installation des tenfold Agent gelten folgende Hardware-Anforderungen:

	Mindestanforderungen
Arbeitsspeicher	8 GB
Festplattenspeicher	10 GB
LAN	GBit

Folgende Betriebssysteme werden für den Betrieb des tenfold Agent unterstützt:

- Microsoft Windows Server 2012®
- Microsoft Windows Server 2012R2®
- Microsoft Windows Server 2016®
- Microsoft Windows Server 2019®
- Microsoft Windows Server 2022®

Hinweis zu .NET für den MSIA

Für den Betrieb des tenfold Agent ist das Microsoft .NET Framework Version 4.8 in der 64-Bit Variante erforderlich.

Tools

Nachfolgende Abschnitte beschreiben Anforderungen hinsichtlich bestimmter Werkzeuge, die zur Einbindung gängiger Systeme hilfreich oder gegebenenfalls erforderlich sind.

Datenbank

Unter Umständen ist es notwendig, auf die Datenbank mittels SQL zuzugreifen, beispielsweise um die ordnungsgemäße Übertragung von Daten aus Fremdsystemen zu kontrollieren. Um dies zu ermöglichen, muss kundenseitig, auf dem für tenfold bereitgestellten Anwendungsserver (oder einem anderen, über Fernwartung erreichbaren System), das jeweilige Datenbank-Tool des gewählten Datenbank-Herstellers installiert werden:

- für Microsoft SQL Server®: Microsoft SQL Server Management Studio®
- für Oracle Database®: Oracle SQL Developer®

Active Directory®

Um die ordnungsgemäße Funktion der Anbindung des Active Directory® zu prüfen, ist es notwendig, dass das Werkzeug "Active Directory® Benutzer und Computer" zur Verfügung steht.

LDAPS

Aus Sicherheitsgründen werden Modifikationen im Active Directory durch tenfold nur über das verschlüsselte Protokoll LDAPS (Port 636) durchgeführt. Stellen Sie daher sicher, dass dieser Dienst zur Verfügung steht.

SAP ERP®

Um die ordnungsgemäße Funktion der Anbindung an SAP® zu prüfen, ist es notwendig, dass die SAP-GUI zur Verfügung steht.

Andere Anwendungen

Für die Einbindung anderer Zielsysteme kann es erforderlich sein, dass die jeweiligen Tools des Herstellers zur Verfügung stehen. Üblicherweise sind dies:

- Datenbanktreiber
- Anwendungs-Clients
- Web-Administrations-Tools

Sollte über diesen Punkt Unklarheit herrschen, ist es zu empfehlen, vorab mit Ihrem Betreuer Kontakt aufzunehmen und eventuelle Erfordernisse abzuklären.

2.1.3 Einrichtung der Dienstkontoen

Vor der Installation müssen folgende Dienstkontoen für tenfold eingerichtet werden:

Beschreibung	Anwendungsfall	Benötigte Berechtigungen
tenfold Application User	Dienstkonto für den Betrieb des Applikationsdienstes	Unter diesem Konto wird der tenfold-Dienst ausgeführt. Dieses Konto wird nur benötigt, wenn der Datenbankzugriff mittels Active Directory-Konto erfolgt. Sollte ein Lokaler Datenbankbenutzer verwendet werden, so läuft der tenfold-Dienst unter "Lokales System". Sollte der tenfold-Dienst unter einem Active Directory-Konto ausgeführt werden, so muss dieses Konto Schreibzugriff auf das tenfold Installationsverzeichnis besitzen.
tenfold Active Directory User	Benutzer- und Berechtigungsmanagement in Active Directory	Lesender und schreibender Zugriff auf das gesamte Active Directory, zum Anlegen von Benutzern, Setzen von Berechtigungen, etc.

Beschreibung	Anwendungsfall	Benötigte Berechtigungen
tenfold File Server Admin	Berechtigungsmanagement auf File Server	Lesender und schreibender Zugriff auf die Verzeichnisse des File Servers, zum Auslesen und Setzen von NTFS-Berechtigungen
tenfold Exchange Admin	Berechtigungsmanagement auf Microsoft Exchange	<p>Lesender und schreibender Zugriff auf den Exchange Server, zum Auslesen und Setzen von Exchange-Berechtigungen. Benötigt eine Mailbox, um öffentliche Ordner auslesen zu können. Muss die Exchange-Rolle "ApplicationImpersonation" besitzen und Mitglied der Active Directory Gruppe "Organization Management" sein.</p> <div> <p>Bitte beachten Sie, dass, je nach Infrastruktur und Exchange Version, die Replikation der Exchange-Berechtigungen bis zu einem Tag dauern kann.</p> </div>
tenfold SharePoint Admin	Berechtigungsmanagement auf Microsoft SharePoint	Lesender und schreibender Zugriff auf den SharePoint Server, zum Auslesen und Setzen von SharePoint-Berechtigungen. Muss Farm Administrator sein.

2.1.4 Port-Freischaltungen

Für den Betrieb von tenfold müssen die unterschiedlichen Komponenten miteinander kommunizieren. Dazu werden bestimmte Port-Freischaltungen benötigt, falls die Systeme durch Firewalls oder Port-Filter geschützt sind. Folgende Freischaltungen sind notwendig:

Quellsystem	Zielsystem	Port	Anmerkung
Endbenutzer (Browser)	tenfold Applikationsserver	8080	Default-Einstellung (kann über Konfiguration angepasst werden)

Quellsystem	Zielsystem	Port	Anmerkung
tenfold Applikationsserver	tenfold Agent	8000	Default-Einstellung (kann über Konfiguration angepasst werden) Die Verbindung wird zu jeder Instanz des tenfold Agent benötigt.
tenfold Applikationsserver	Mail Server	25	Für den Versand von E-Mails benötigt tenfold Zugang zu einem internen SMTP Server
tenfold Applikationsserver	Datenbankserver	1433 (SQL Server) 1521 (Oracle)	Diese Verbindung wird für den Zugriff von tenfold auf das genutzte Datenbanksystem benötigt. Bei den angegebenen Ports handelt es sich um die Default-Ports der jeweiligen Hersteller. Wenn diese Default-Einstellung geändert wurde, so müssen die jeweils tatsächlich genutzten Ports freigeschalten werden.
tenfold Applikationsserver	tenfold Marketplace	HTTPS	Diese Verbindung ist zum Installieren und Aktualisieren der verwendeten Plugins erforderlich.
tenfold Applikationsserver	Active Directory	389 (ldap), 636 (ldaps)	Die Verbindung wird zur Verbindung mit dem Active Directory benötigt. Diese Verbindung muss vom tenfold Applikationsserver zu zumindest einem Domaincontroller jeder einzurichtenden Domain hergestellt werden können.
tenfold Agent	tenfold Applikationsserver	61613	Diesen Port benutzt der tenfold Agent, um die Ergebnisse der Scans (Filserver, Exchange, Microsoft 365, etc) an tenfold zu senden.

Microsoft 365

Für die Anbindung an Microsoft 365 müssen sowohl der tenfold Server als auch der tenfold Agent Zugang zu folgenden externen Hosts der Microsoft Graph API haben:

- login.microsoftonline.com²
- graph.microsoft.com³

Für eine Exchange Online-Anbindung ist Zugriff auf folgende URLs der Microsoft 365 Cloud erforderlich:

- <https://www.office.com>
- <https://outlook.office365.com/Powershell-LiveID>
- <https://outlook.office365.com/EWS/Exchange.asmx>

Graph API

Die hier angeführte Liste kann sich seitens Microsoft zu jedem Zeitpunkt ändern. Bei Problemen kann unter <https://docs.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide> eine vollständige und tagesaktuelle Liste alle Microsoft 365 URLs eingesehen werden.

Weiters benötigt der Agent eine Installation folgender PowerShell-Module:

Module

```
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
# Benötigt für Exchange Online
Install-Module -Name ExchangeOnlineManagement -RequiredVersion 3.1.0 -Force
# Benötigt für SharePoint Online
Install-Module -Name PnP.PowerShell -RequiredVersion 1.9.0
```

Für die Funktion dieser PowerShell-Module müssen, laut Microsoft, die Ports 80 (HTTP) und 443 (HTTPS) freigeschalten sein.

HTTP

Da Microsoft den Port 80 aufführt wird dieser hier ebenso aufgeführt, obwohl die Kommunikation normalerweise über den HTTPS-Port stattfindet. Eine Dokumentation über die interne Arbeitsweise der Module, die offenlegt, wofür und warum der Port 80 gebraucht werden sollte, existiert seitens Microsoft nicht.

2.2 Anlegen der Datenbank

Datensicherheit

In der tenfold Datenbank werden kritische Informationen gespeichert. Darunter befinden sich zum einen personenbezogene Daten, die, je nach anwendbaren Gesetzen, besonders geschützt werden müssen und zum anderen sensible Systemeinstellungen, wie Credentials für Systemkonten mit hohen administrativen Rechten, die tenfold zum Zugriff auf Fremdsysteme benötigt. Es ist daher ein dem Stand der Technik ausreichender Schutz der Datenbank mittels sicherer Authentifizierung und gegebenenfalls Verschlüsselung zu wählen.

² <https://login.microsoftonline.com>

³ <https://graph.microsoft.com>

2.2.1 Allgemeine Hinweise

tenfold nutzt die Datenbank, um alle Daten zu Benutzern und Berechtigungen zu speichern. Bis auf wenige Ausnahmen sind auch alle Systemeinstellungen in der Datenbank gespeichert. Aktuell werden von tenfold folgende Datenbanksysteme unterstützt:

- Microsoft SQL Server
- Oracle Database

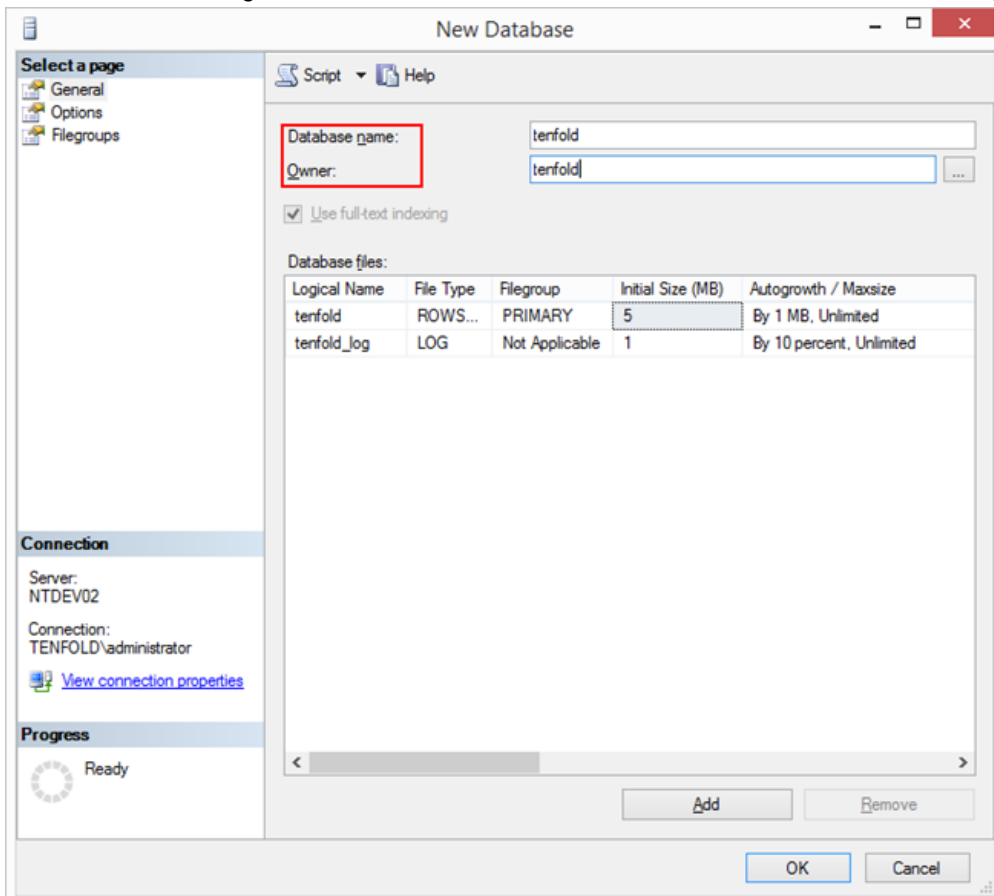
2.2.2 Anlegen einer Microsoft SQL Server Datenbank

Es stehen Ihnen zwei Möglichkeiten zur Verfügung:

- Installation eines neuen Microsoft SQL Servers (siehe <https://docs.microsoft.com/en-us/sql/database-engine/install-windows/install-sql-server?view=sql-server-2017>)
- Nutzung eines bestehenden Microsoft SQL Servers

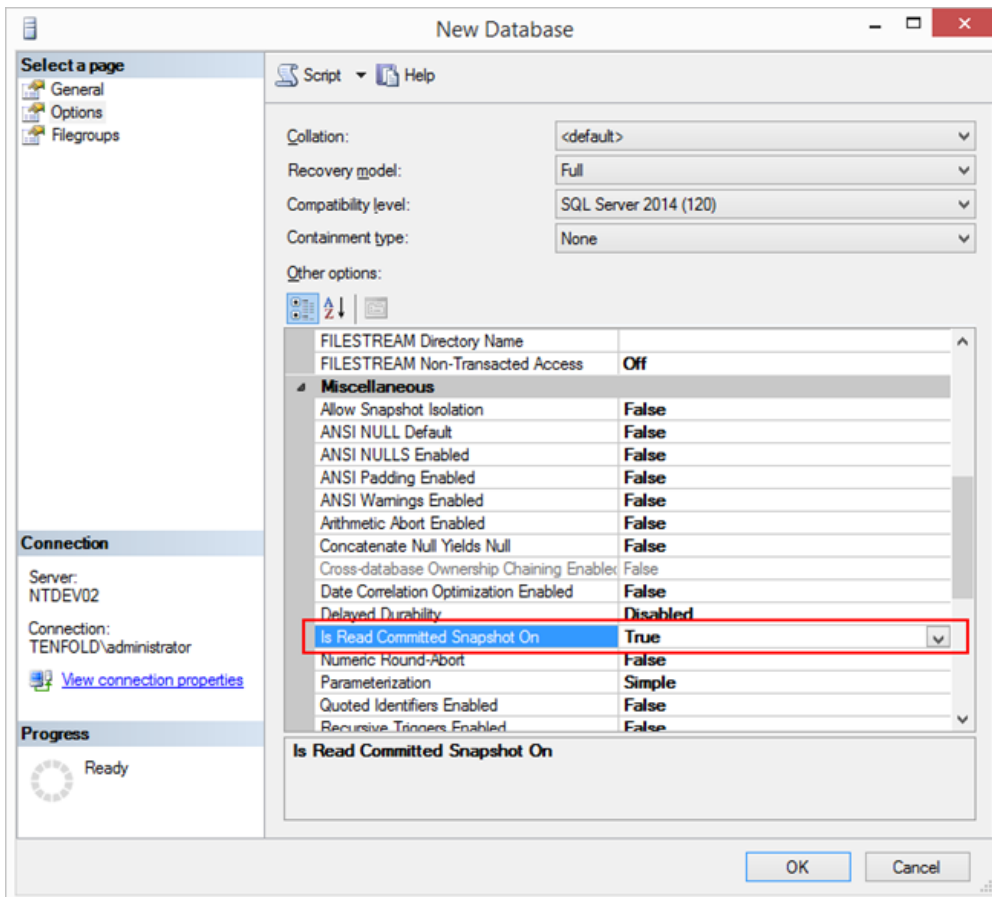
Nachdem Sie den SQL Server bereitgestellt haben, nutzen Sie das Microsoft SQL Management Studio, um eine neue Datenbank anzulegen. Für den Zugriff auf die Datenbank sollten Sie ein entsprechendes Konto anlegen. Es werden von tenfold sowohl SQL-Server-Benutzer, als auch Active Directory-Benutzer unterstützt.

- Geben Sie der Datenbank den Namen "tenfold".
- Legen Sie das zuvor angelegte Konto schließlich als Eigentümer für die neue Datenbank fest.
- Die Einstellungen für die Datenbankdateien können auf den Default-Einstellungen belassen werden.



Option

Die Option "Is Read Committed Snapshot On" muss anschließend unbedingt auf den Wert "True" gesetzt werden. tenfold wird ohne diese Einstellung nicht ordnungsgemäß funktionieren.



Anschließend kann die Datenbank angelegt werden.

2.2.3 Anlegen einer Oracle Datenbank

Es stehen Ihnen zwei Möglichkeiten zur Verfügung:

- Installation eines neuen Oracle Database Servers (siehe http://www.oracle.com/webfolder/technetwork/tutorials/obe/db/12c/r1/Windows_DB_Install_OBE/Installing_Oracle_Db12c_Windows.html)
- Nutzung eines bestehenden Oracle Database Servers

Zeichensatz

tenfold erfordert in nahezu allen Fällen, dass der Zeichensatz der Datenbank "AL32UTF8" ist. Sie können den Zeichensatz der aktuellen Datenbank über folgenden Befehl in SQL*Plus verifizieren:
`SELECT value FROM v$nls_parameters WHERE parameter LIKE 'NLS_CHARACTERSET';`

Die Ausgabe muss "AL32UTF8" lauten. Weicht die Ausgabe ab, so muss eine Datenbank mit dem passenden Zeichensatz zur Verfügung gestellt werden.

Nachdem Sie den Oracle Database Server bereitgestellt haben, nutzen Sie SQL*Plus, um anschließend ein neues Benutzerschema anzulegen, welches Sie "tenfold" nennen. Der Benutzer benötigt Berechtigungen, um in seinem Schema Objekte (Tabellen, Views, etc.) anlegen, ändern und löschen zu können.

2.3 Ausführung des Installationsassistenten

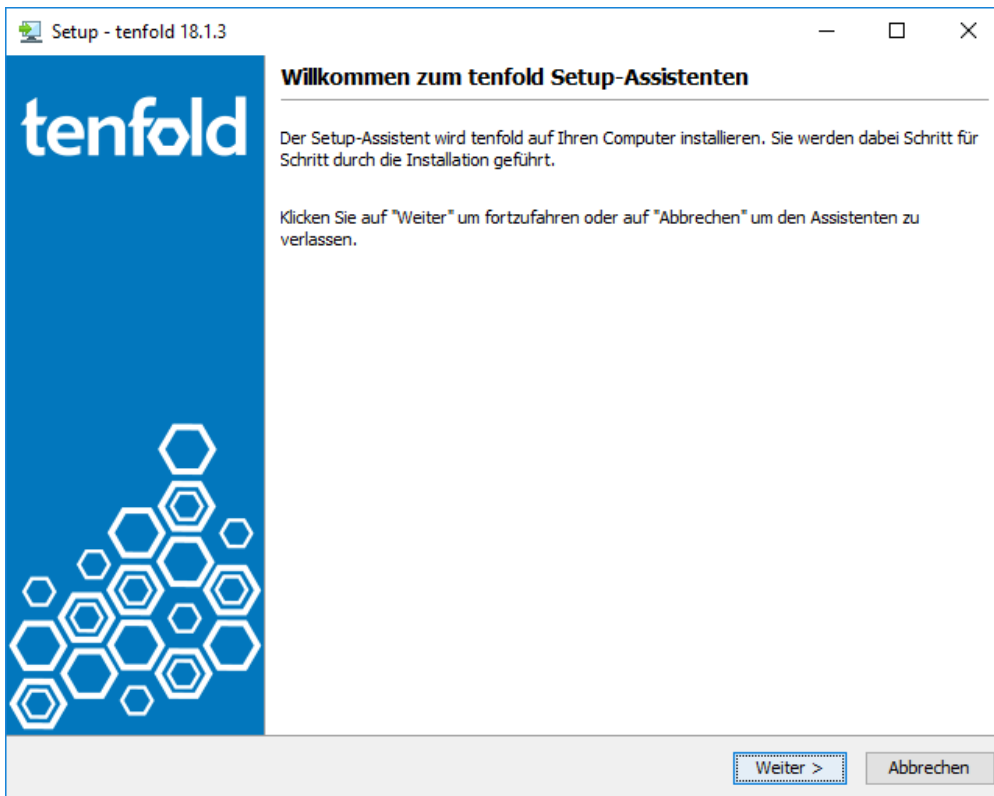
2.3.1 Voraussetzungen

Für die Ausführung gelten folgende Voraussetzungen:

- Sie haben die Installationsdatei (zum Beispiel "tenfold_windows-x64_18_1_3") von [tenfold Connect](https://connect.tenfold-security.com)⁴ heruntergeladen
- Es steht ein Microsoft Windows Server bereit (für die unterstützten Versionen siehe [Systemvoraussetzungen](#)(see page 26))
- Sie haben sich auf dem Server mit Administrationsrechten angemeldet

2.3.2 Start

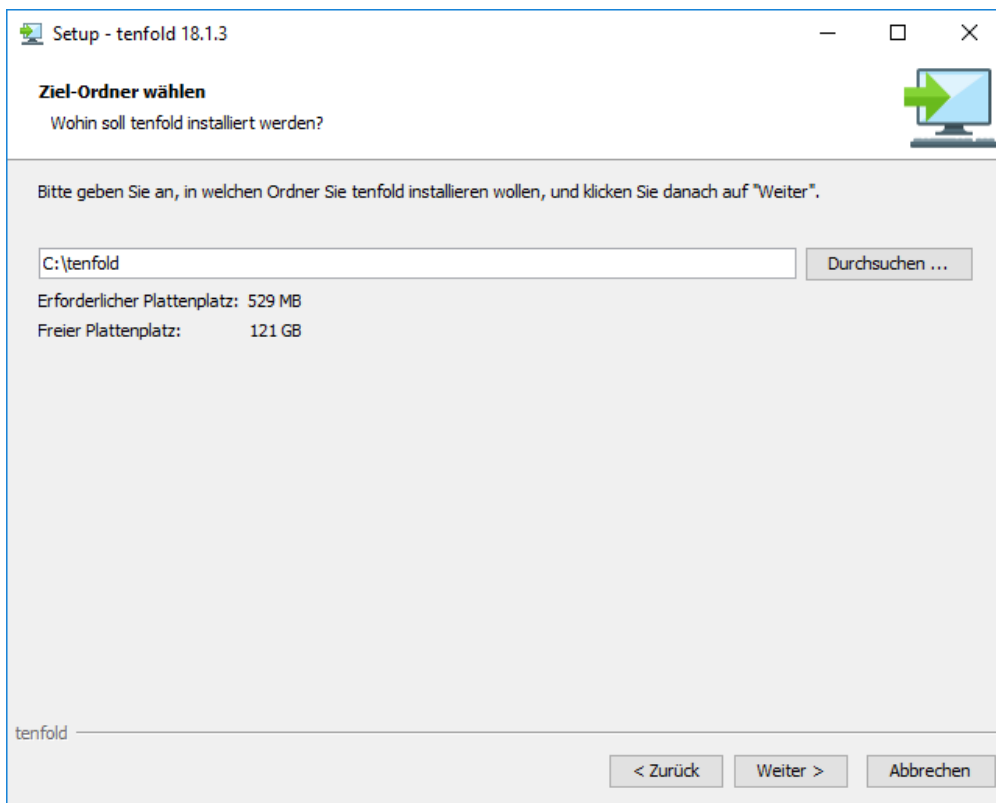
Führen Sie die Installationsdatei aus. Es startet nun der Assistent. Klicken Sie auf "Weiter".



2.3.3 Zielordner wählen

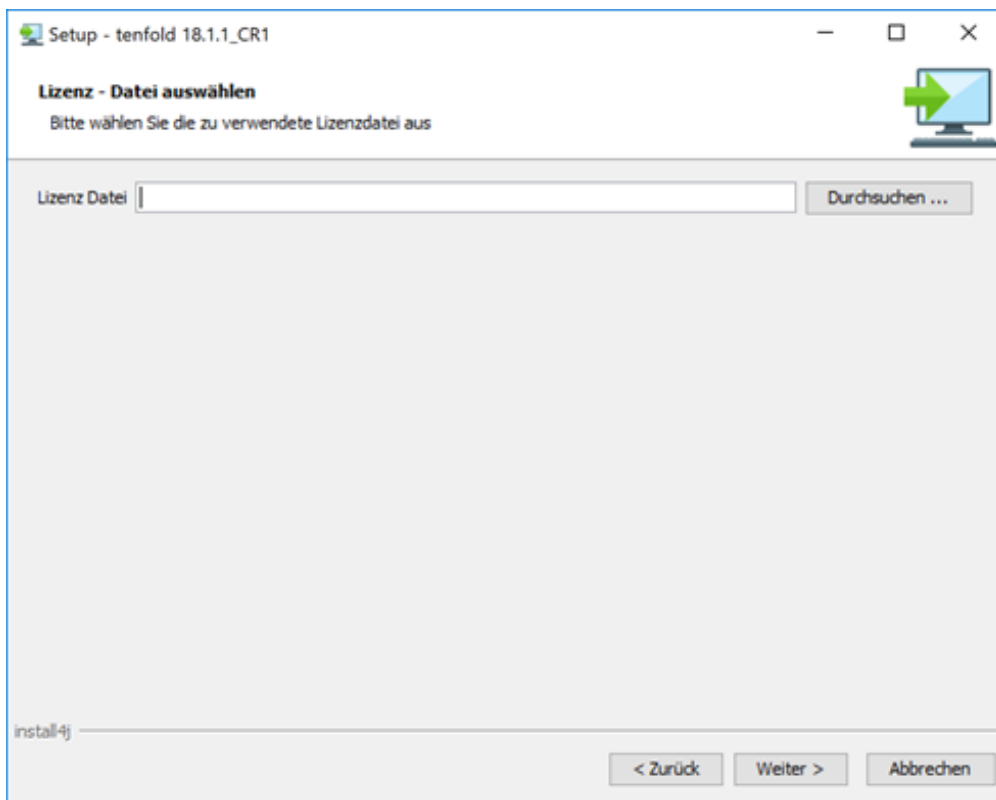
Im ersten Schritt müssen Sie den Zielordner für die tenfold-Programmdateien auswählen. Klicken Sie anschließend auf "Weiter".

⁴ <https://connect.tenfold-security.com>



2.3.4 Einspielen der Softwarelizenz

Für die Nutzung von tenfold benötigen Sie eine entsprechende Softwarelizenz. Diese wird Ihnen von Ihrem Händler oder direkt vom Hersteller in Form einer Datei zur Verfügung gestellt. Sie müssen nun diese Lizenzdatei auswählen. Klicken Sie anschließend auf "Weiter".



Konfiguration der Datenbankverbindung

Da tenfold bereits im Rahmen des Installationsassistenten Einstellungen in der Datenbank vornimmt, müssen Sie nun die Verbindungsdaten bekanntgeben:

Legen Sie die folgenden Einstellungen fest:

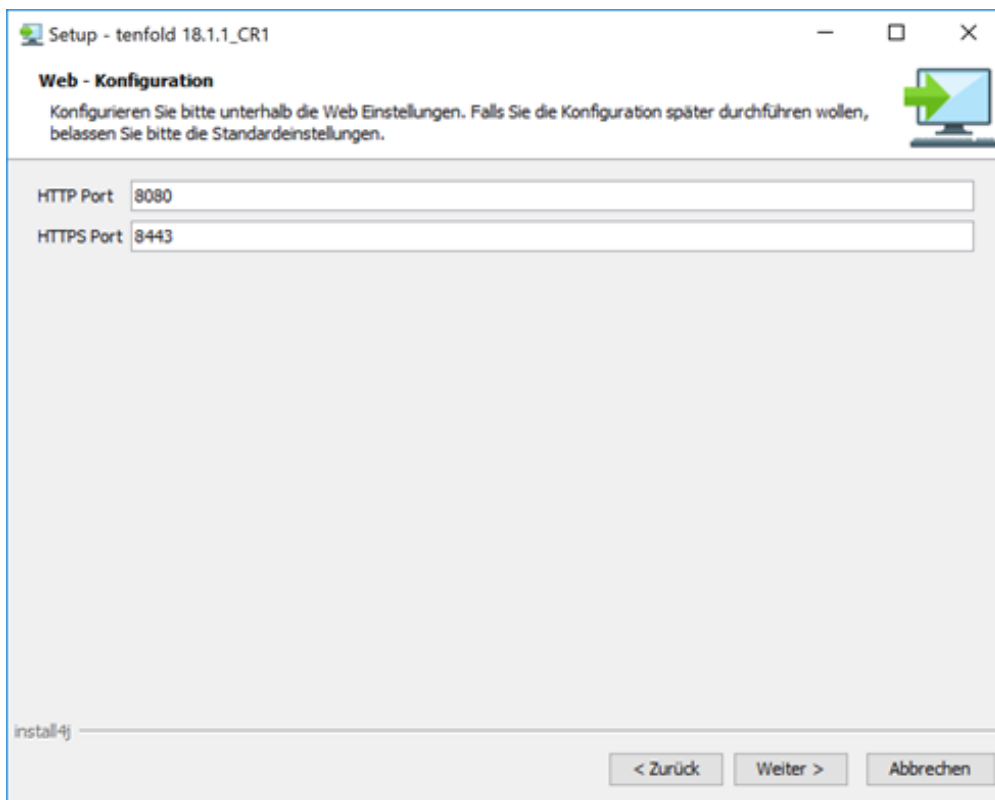
- Host: Hostname des Datenbankservers
- Instanz: Instanzname der Datenbank (nur Microsoft SQL Server)
- Port: 1433 (Microsoft SQL Server Default) oder 1521 (Oracle Database Default).
- Wenn statt eines fixen Port "Dynamic Ports" genutzt werden sollen, setzen Sie das Häkchen.
- Benutzername: Benutzername des Datenbankbenutzers
- Passwort: Das Passwort des Benutzers
- Erweiterte Parameter: Dieses Feld ist eine Experteneinstellungen und sollte leer bleiben.

SQL Server-Benutzer und Active Directory-Benutzer

Wenn Sie beim Anlegen der Datenbank als Eigentümer einen SQL Server-Benutzer ausgewählt haben, so geben Sie dessen Daten in "Benutzername" und "Passwort" ein. Wenn Sie bei der Anlage dagegen einen Active Directory-Benutzer gewählt haben, so geben Sie diesen in "Benutzername" in der Form DOMAIN\Benutzername ein. Das Passwort des Active Directory-Benutzers geben Sie in "Passwort" ein. Wenn Sie einen Active Directory-Benutzer gewählt haben, so konfiguriert der Assistent den tenfold Dienst anschließend so, dass dieser unter genau diesem, für die Datenbank gewählten Benutzer, läuft. Das garantiert, dass der Dienst (über NTLM authentifiziert) anschließend auf die Datenbank zugreifen kann. Haben Sie einen SQL Server-Benutzer gewählt, so konfiguriert der Assistent den Dienst so, dass dieser unter "LOCAL SYSTEM" läuft. Die Authentifizierung des Dienstes gegenüber der Datenbank erfolgt dann über Benutzername und Passwort.

2.3.5 Festlegen der Web-Ports

tenfold ist eine 100% webbasierte Lösung, die über einen Browser bedient wird. In diesem Schritt können Sie festlegen, auf welchen Ports der tenfold-Server auf eingehende HTTP und HTTPS-Verbindungen warten soll.



Ports

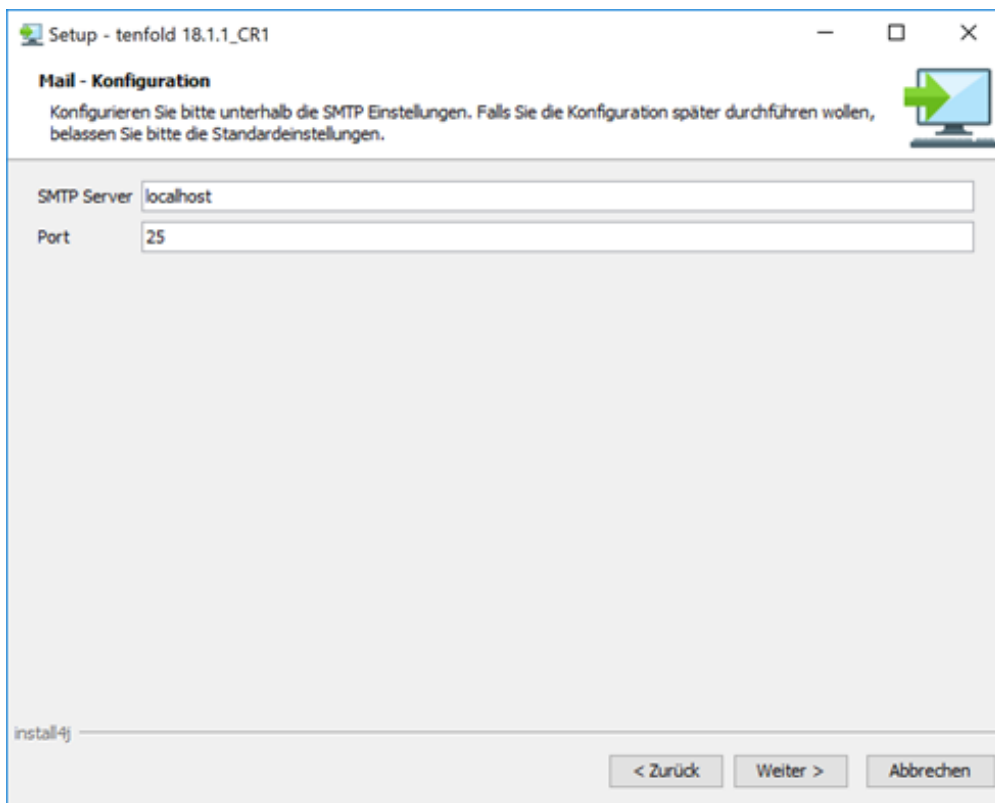
Der Betrieb von tenfold wird nur auf dezidierten Servern unterstützt. Das bedeutet, dass auf dem gleichen Server keine anderen Dienste (mit Ausnahme der Windows-Standarddienste) betrieben werden dürfen. Kontrollieren Sie dennoch, dass die gewünschten Ports von keinem anderen Programm genutzt werden. Sie können dies mit dem Befehl "netstat" überprüfen:

```
netstat -ano | find "8080"
```

```
netstat -ano | find "8443"
```

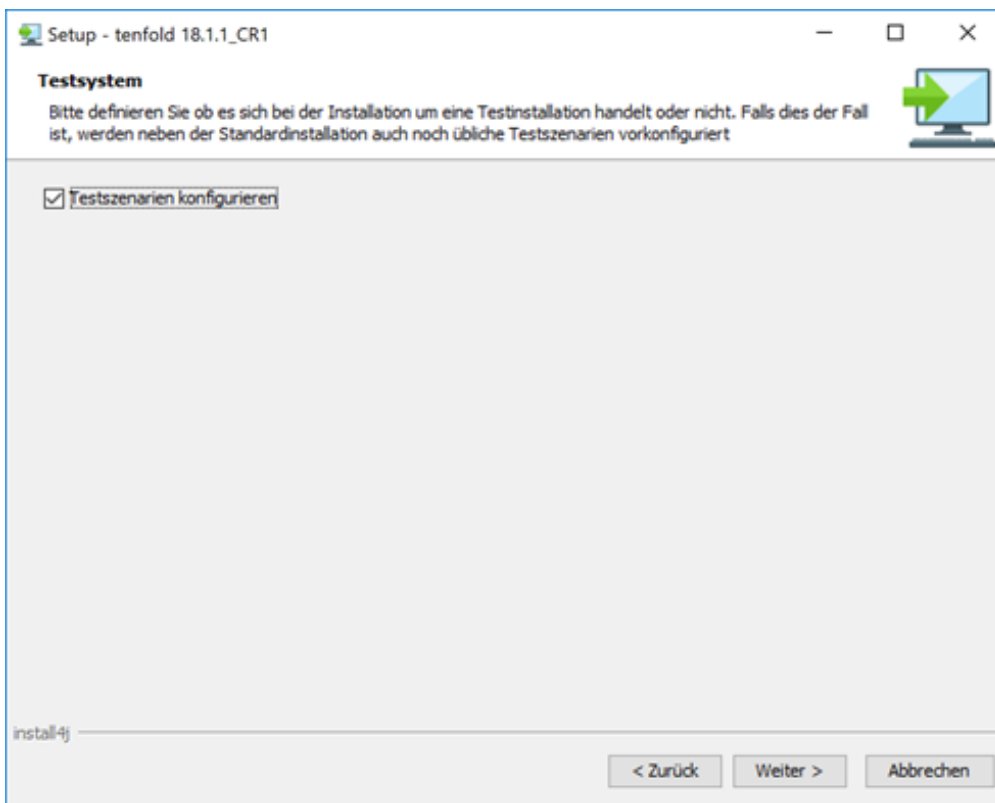
2.3.6 Festlegen des SMTP-Servers

tenfold nutzt SMTP, um E-Mail-Benachrichtigungen, Berichte und andere Informationen an Benutzer zu versenden. Legen Sie in diesem Schritt Ihren SMTP-Server fest.



2.3.7 Testszenarien

Abhängig von der tenfold-Version folgt der Schritt "Testsystem". Setzen Sie hier - unabhängig, ob es sich um eine Test- oder Produktivinstallation handelt - in jedem Fall das Häkchen. Es werden hierbei wertvolle Basiseinstellungen und Stammdaten angelegt, die anschließend nicht mehr manuell angelegt werden müssen.



2.3.8 Kopieren der Dateien und Abschluss

Der Assistent kopiert anschließend die Programmdateien in das Programmverzeichnis. Danach ist die Installation abgeschlossen.

2.4 Installation des tenfold Agent

2.4.1 Aufgaben des tenfold Agent

Der tenfold Agent ist ein eigenständiger Dienst, der notwendig ist, um wesentliche Bestandteile der Microsoft-Systemlandschaft in tenfold einzubinden. Dazu zählen:

- Einlesen der Fileserver-Berechtigungen
- Einlesen der Microsoft 365-Mandanten
- Einlesen der Exchange Server-Berechtigungen
- Einlesen der SharePoint-Berechtigungen
- Ausführung von PowerShell-Scripts

Der tenfold Agent muss installiert und anschließend in tenfold registriert werden. Pro Umgebung können grundsätzlich beliebig viele tenfold Agents installiert werden, die anschließend in tenfold eingebunden werden. Wann und wo die Installation eines tenfold Agent empfehlenswert ist, können Sie unter [Einrichten des tenfold Agent](#) (see page 199) nachlesen. Eine Installation des Agent auf dem tenfold Server ist grundsätzlich immer empfehlenswert. Sollte dieser Agent entweder überlastet sein (weil ein Fileserver in entfernten Niederlassung eingelesen werden muss) oder vereint das für den tenfold Agent-Dienst konfigurierte Dienstkonto nicht alle benötigten Berechtigungen für die gestellten Aufgaben (zum Beispiel Vollzugriff-Berechtigungen auf dem Fileserver und administrative Berechtigungen in Exchange Server), so muss die Installation weiterer Agents in Angriff genommen werden.

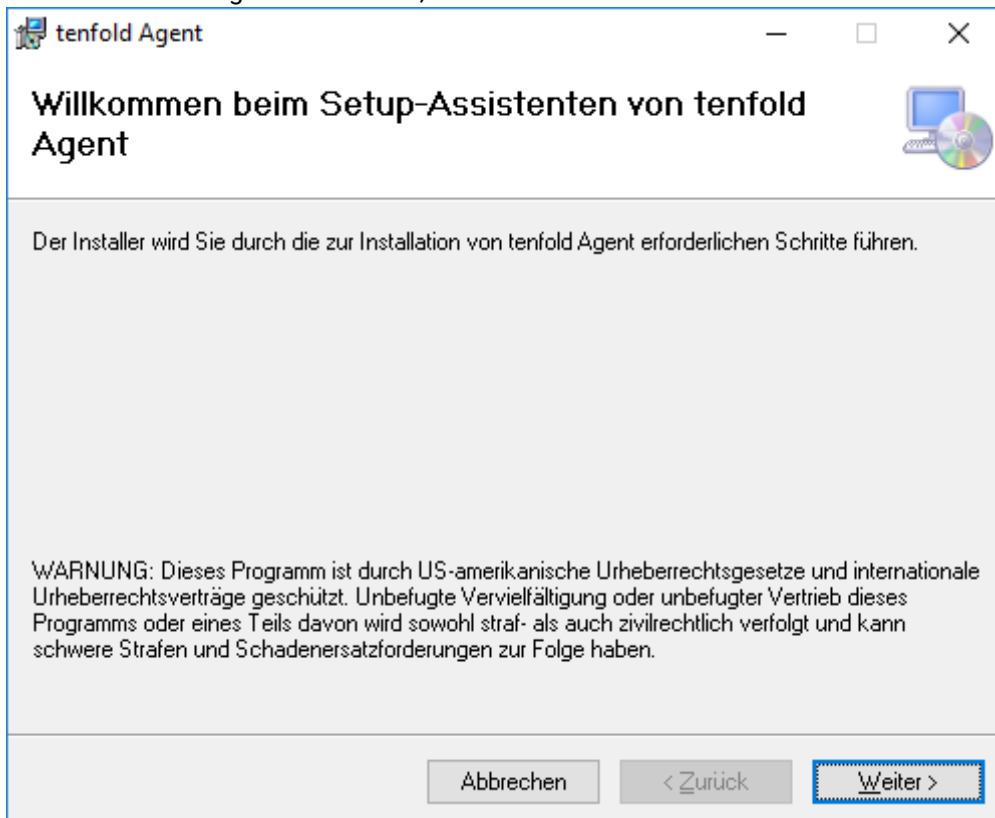
2.4.2 Installation

Berechtigungen

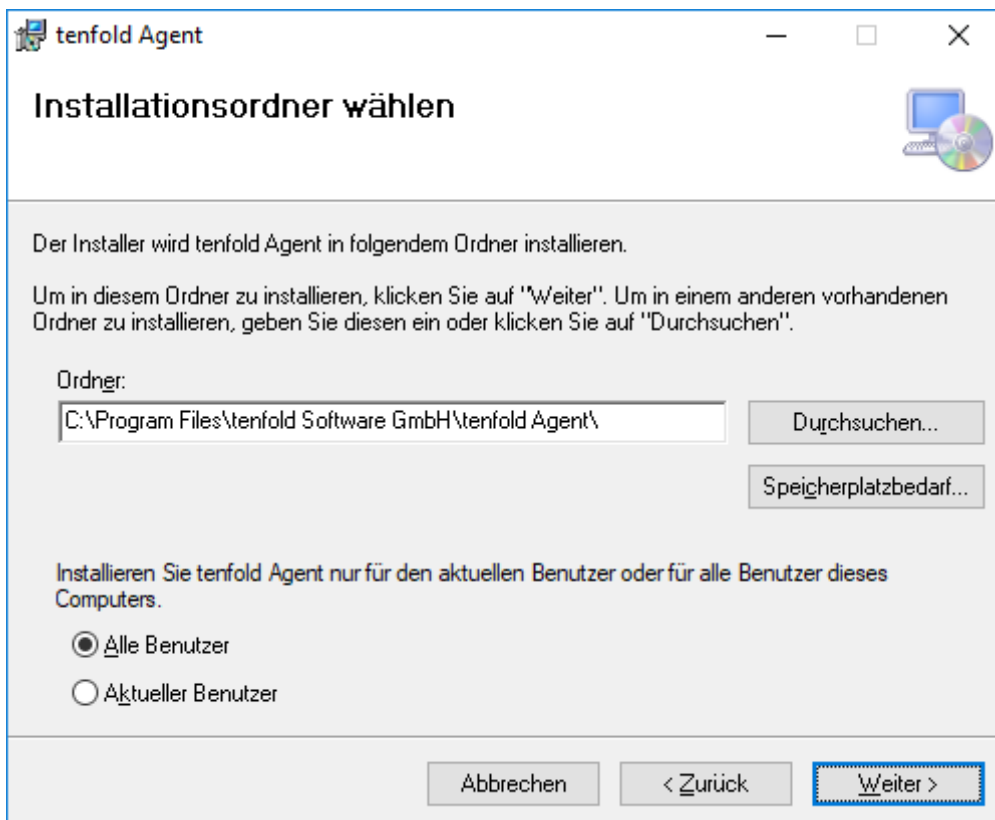
Beachten Sie, dass zur Installation des tenfold Agent lokale Administrationsrechte auf dem Zielsever erforderlich sind.

Um den tenfold Agent initial zu installieren, lokalisieren Sie die Setup-Datei, die mit der tenfold-Installation geliefert wurde aus. Diese befindet sich unter C:\tenfold\setup\agents (wenn Sie tenfold unter C:\tenfold installiert haben) und hat beispielsweise den Namen tenfold-agent-18_1_2.msi.

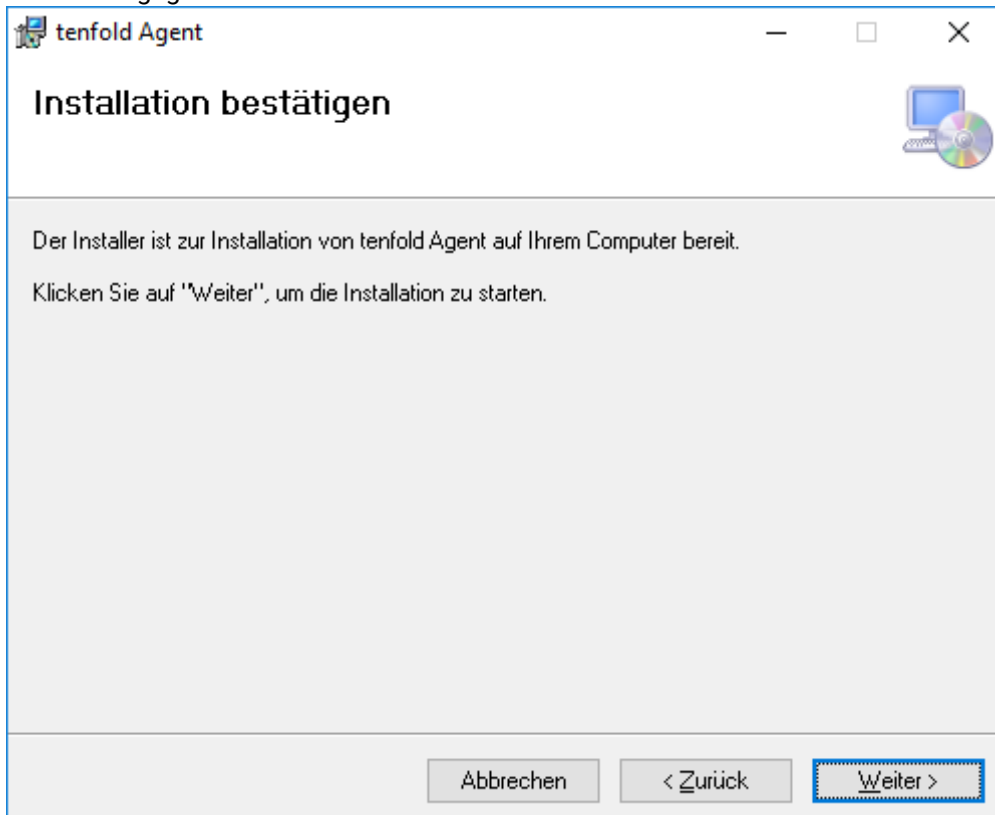
Wenn Sie die Datei gefunden haben, so führen Sie diese aus.



Klicken Sie auf "Weiter".



Ändern Sie gegebenenfalls das Installationsverzeichnis und klicken Sie auf "Weiter".



Klicken Sie erneut auf "Weiter". Die Installation wird anschließend durchgeführt.

2.4.3 Dienstanmeldung

Es erscheint ein Eingabefenster, in welchem die Anmeldeinformationen für das Dienstkonto eingegeben werden müssen, unter welchem der tenfold Agent laufen soll. Es muss berücksichtigt werden, dass je nach Aufgabe, die der tenfold Agent anschließend übernehmen soll, der Benutzer, der verwendet wird, über die entsprechenden administrativen Berechtigungen verfügen muss. Hat der Benutzer beispielsweise keine "Vollzugriff"-Berechtigungen auf dem Fileserver, so kann dieser Agent nicht für die Verwaltung der Fileserver-Berechtigungen verwendet werden, bis der Benutzer nicht mit den entsprechenden Berechtigungen ausgestattet wurde.

Wenn Sie die Informationen eingegeben haben, wird der Dienst auf dem Server registriert. Er scheint anschließend in der Dienstverwaltung als "tenfold Agent" auf.

Telefondienst	Verwaltet den Telefoniestatus des Geräts.	Manuell...	Lokaler Dienst
Telefonie	Bietet Telefonie-API-Unterstützung (TAPI) für Programme, die lokale un...	Manuell	Netzwerkdienst
tenfold Agent	tenfold Agent for Microsoft Infrastructure	Wird au...	Automa... prod\svc-tenfold-fs
tenfold Server	tenfold Application Server	Wird au...	Automa... PROD\svc-tenfold
Überwachung verteilter Ver	Hält Verknüpfungen für NTFS-Dateien auf einem Computer oder zwisch	Wird au...	Automa... Lokales System

Anschließend muss der Agent in tenfold registriert werden. Dieser Vorgang wird in [Einrichten des tenfold Agent](#) (see page 199) beschrieben.

3 Grundfunktionen

3.1 Systemaufbau und Begriffe

In diesem Kapitel werden die grundlegenden Objekte und Zusammenhänge in tenfold beschrieben. Alle nachfolgenden Abschnitte beziehen sich auf die hier aufgeführten Begriffe.

3.1.1 Organisatorischer Aufbau

Personen

Das primäre Objekt in tenfold ist die "Person". Eine Person entspricht üblicherweise (mit wenigen Ausnahmen) einem physischen Menschen. Die Person kann dabei entweder ein Angestellter des Unternehmens, oder ein externer (bei einem anderen Unternehmen beschäftigter) Mitarbeiter sein. Eine Person darf nicht verwechselt werden mit einem Benutzerkonto in einem IT-System. Einer Person können mehrere IT-Benutzer (mitunter in unterschiedlichen Systemen) zugeordnet sein. Die IT-Benutzerkonten werden im System als Zuordnungen von Ressourcen zur Person dargestellt.

Die Stammdaten einer Person bestehen aus einem oder mehreren Sets an Werten zu bestimmten Attributen. Diese Sets werden in weiterer Folge auch als "Stammdatensätze" einer Person bezeichnet. Welche Attribute für eine Person gepflegt werden können (und müssen) wird in der Personenart definiert. Jede Person ist genau einer Personenart zugeordnet. Die Stammdaten einer Person werden in der Datenbank historisiert

gespeichert. Änderungen an den Stammdaten sind nur über einen Request möglich. Jede Änderung an Attributen (in weiterer Folge auch als "Personenfelder" bezeichnet) erzeugt einen neuen Stammdatensatz. Der zuvor gültige Stammdatensatz wird historisiert.

Häufig wird einer Person nur ein Stammdatensatz zugeordnet. Diese Vorgehensweise ist dann praktikabel, wenn die Person genau einer Abteilung, einem Standort, einer Position, usw. zugeordnet wird. Ist eine Person jedoch parallel in mehreren Abteilungen und Niederlassungen des Unternehmens tätig, und hat sie eventuell aufgrund dessen mehrere Telefonnummern oder Mobilnummern, so müssen für diese Person mehrere Stammdatensätze angelegt werden.

Unternehmen

Unternehmen bilden die einzelnen Gesellschaften des Unternehmens ab. Besteht ein Unternehmen lediglich aus einer Gesellschaft, so existiert in tenfold dementsprechend auch nur ein Unternehmen. Unternehmen können hierarchisch organisiert sein, indem einem Unternehmen das jeweilige übergeordnete Unternehmen zugeordnet wird. Ein Unternehmen ist einer Person niemals direkt, sondern über eine Niederlassung zugeordnet.

Niederlassungen

Eine Niederlassung entspricht dem physischen Standort (Anschrift) eines Unternehmens (einer Gesellschaft). Ein Unternehmen kann somit über mehrere Niederlassungen verfügen. Eine Anschrift kann gleichzeitig mehrere Unternehmen beherbergen.

Einer Person können - je nach Einstellung in der Personenart - innerhalb eines Stammdatensatzes eine oder mehrere Niederlassungen zugeordnet werden. Eine der Niederlassungen wird dabei als "Hauptniederlassung" festgelegt. Die Hauptniederlassung bildet dabei in den meisten Fällen die steuernde Niederlassung.

Beispielsweise werden die Adressdaten (Straße, PLZ, Ort usw.) in Fremdsystemen üblicherweise mit den Daten der Hauptniederlassung (und nicht mit den Daten einer anderen Niederlassung) befüllt.

Niederlassungen werden in Profilen häufig als Steuerungsattribut genutzt, um bestimmte lokale Ressourcen automatisch zuzuordnen (z.B. die Mailverteilergruppe für den Standort)

Gebäude

Einer Person kann ein Gebäude zugeordnet werden. Gebäude selbst werden bestimmten Niederlassungen zugeordnet. Gebäude können sowohl aus Gründen der Stammdatenpflege (z.B. Übertragung der Gebäudebezeichnung in ein Attribut im Active Directory), als auch aus steuernden Gründen hinterlegt sein (z.B. automatische Zuordnung von Profilen).

Abteilungen

Abteilungen bilden die unterschiedlichen Bereiche des Unternehmens ab. Abteilungen können hierarchisch organisiert sein, indem einer Abteilung die jeweilige übergeordnete Abteilung zugeordnet wird. Parallel zur Abteilungshierarchie ist jede Abteilung einer Abteilungsgruppe zugeordnet. Jede Person kann pro Stammdatensatz einer Abteilung zugeordnet werden. Eine Abteilung kann auf bestimmte Niederlassungen beschränkt werden (die Abteilung "IT" ist vielleicht nur in der Zentrale zu finden). Es stehen dann nur die Abteilungen zur Auswahl, die entweder zur Niederlassung im gleichen Stammdatensatz passen, oder die keine Beschränkung auf bestimmte Niederlassungen haben. Über Profile werden häufig auf Basis der Abteilung die Zuordnung von Ressourcen und Berechtigungen gesteuert.

Abteilungsgruppen

Zur Gruppierung von Abteilungen gleicher Art können Abteilungsgruppen verwendet werden. Abteilungen können Abteilungsgruppen unabhängig von deren Position in der Hierarchie zugeordnet werden. Der Zweck von Abteilungsgruppen ist üblicherweise die Gruppierung gleichartiger Abteilungen zum Zweck der Zuordnung von Ressourcen und Berechtigungen über Profile sowie zur Nutzung als Filterkriterium auf

bestimmten Masken. Eine Person ist einer Abteilungsgruppe nie direkt, sondern über die zugehörigen Abteilungen zugeordnet.

Positionen

Eine Position bildet eine bestimmte Stelle im Unternehmen ab (z.B. "Verkäufer Ersatzteile Innendienst"). Einer Person kann pro Stammdatensatz eine Position zugeordnet werden. Eine Position kann auf bestimmte Abteilungen beschränkt werden (die Position "Verkäufer Ersatzteile Innendienst" ist gegebenenfalls nur in der Abteilung "Verkauf" zu finden). Es stehen dann nur die Positionen zur Auswahl, die entweder zur Abteilung im gleichen Stammdatensatz passen, oder die keine Beschränkung auf bestimmte Abteilungen haben.

Organisationseinheiten

Die Organisationseinheit stellt die technische Konfiguration hinsichtlich des Active Directory für eine bestimmte Niederlassung dar. In der Organisationseinheit werden unter anderem die Active Directory-Domäne, die Active Directory-OE für Benutzer sowie der Pfad zum lokalen Fileserver konfiguriert. Da es mehrere Niederlassungen mit der gleichen technischen Konfiguration geben kann (z.B. Niederlassungen unterschiedlicher Unternehmen am gleichen Standort), wird jeder Niederlassung eine Organisationseinheit zugeordnet.

Organisationseinheitsgruppen

Zur Gruppierung können Organisationseinheiten in Organisationseinheitsgruppen gruppiert werden. Diese dienen lediglich zur einfacheren Auswahl, z.B. als Filterkriterium auf einigen Masken.

Kostenstellen

Kostenstellen können in tenfold hinterlegt werden, um sie einer Person direkt zuzuordnen. Kostenstellen können dabei sowohl aus Gründen der Stammdatenpflege (z.B. Übertragung der Kostenstellennummer in ein Attribut im Active Directory), als auch aus steuernden Gründen hinterlegt sein (z.B. automatische Zuordnung von Profilen auf Basis der Kostenstelle). Ein weiterer Anwendungsfall ist das Mapping von Kostenstellen auf Abteilungen im Falle der Übernahme von Daten aus Personalmanagementsystemen (häufig werden dort lediglich Kostenstellen bereitgestellt, die dann auf Seite von tenfold auf Abteilungen umgewandelt werden).

Ressourcen

Ressourcen stellen in tenfold einen einer Person zuordnungsfähigen Artikel dar. In den meisten Fällen stellen Ressourcen bestimmte Anwendungen dar. Durch Zuordnung der Ressource zur Person entsteht üblicherweise ein Benutzerkonto für die Person in der jeweiligen Anwendung. Durch Sperre der Ressourcenzuordnung wird das Konto dann entsprechend gesperrt. Analog verhält es sich bei Stammdatenänderungen, Löschungen und Sperre/Entsperrung.

Grundsätzlich können aber alle Artikel, die einer Person zugeordnet werden können als Ressource abgebildet werden. Dazu zählt zum Beispiel auch Hardware oder bestimmte IT-Funktionen, wie beispielsweise Internetzugang oder VPN-Zugang. In der Konfiguration der Ressource ist hinterlegt, wie diese für die Person bereitgestellt (provisioniert) wird. Dies erfolgt durch Angabe des gewünschten EXEC. Über die unterschiedlichen Scripts, die im EXEC hinterlegt sind, wird gesteuert, was bei der Anlage, Änderung, Sperre, Löschung, etc. zu passieren hat.

Ressourcen können Bestandteil von Profilen sein.

Anwendungsberechtigungen

Anwendungsberechtigungen stellen eine Berechtigung in einem angebundenen Fremdsystem dar (ausgenommen davon sind lediglich Active Directory-Gruppen, welche speziell behandelt werden). Beispielsweise wird eine SAP-Rolle, aber auch eine Gruppe in IBM Notes in tenfold als

Anwendungsberechtigung dargestellt. Anwendungsberechtigungen sind immer einer Ressource zugeordnet, wobei die Ressource das System selbst darstellt. Durch Zuordnung der Ressource erhält die Person das gewünschte Benutzerkonto (ohne Berechtigungen) und durch Zuordnung der Anwendungsberechtigungen werden die entsprechenden Rollen und Gruppen dem Benutzerkonto zugeordnet.

Anwendungsberechtigungen können Bestandteil von Profilen sein.

Active Directory-Gruppen

Active Directory-Gruppen stellen üblicherweise Berechtigungen in der Microsoft-Umgebung dar. Sie werden in tenfold speziell behandelt und nicht als Anwendungsberechtigungen abgebildet. Diese spezielle Behandlung ist aufgrund der tiefgehenden Integration von tenfold mit dem Active Directory notwendig. Active Directory-Gruppen haben in tenfold beispielsweise eine Reihe von Attributen (SID, GUID, Domäne, Organisationseinheit), welche für Anwendungsberechtigungen nicht vorgesehen sind. tenfold kennt außerdem die Zusammenhänge zwischen den Active Directory-Gruppen. tenfold weiß somit, welche Benutzer in welchen Gruppen und welche Gruppen in welchen Gruppen Mitglied sind. Diese Informationen sind über Domänengrenzen hinweg vorhanden. Sie sind Voraussetzung für die Reportingfunktionen, die tenfold für Active Directory basierte Systeme (Fileserver, Exchange, SharePoint) zur Verfügung stellt.

Active Directory-Gruppen können Bestandteil von Profilen sein.

Profile

Profile gruppieren Objekte systemübergreifend (Ressourcen, Anwendungsberechtigungen, Active Directory-Gruppen) nach bestimmten Merkmalen und ermöglichen die gleichzeitige Zuordnung aller enthaltenen Objekte zu einer Person. Das vereinfacht und beschleunigt den Prozess zur Bereitstellung von Berechtigungen in mehreren Systemen. Profile können Personen manuell zugeordnet werden. Jede Person kann kein, ein oder mehrere Profile gleichzeitig zugeordnet haben.

Profile beinhalten außerdem Regeln zur automatischen Zuordnung auf Basis von Feldregeln. Damit lässt sich steuern, dass Profile bei Auftreten bestimmter Attribute in einem der Stammdatensätze einer Person automatisch zugewiesen werden. Somit lassen sich Ressourcen, Anwendungsberechtigungen und Active Directory-Gruppen automatisch einer Person zuordnen, wenn diese beispielsweise einer bestimmten Abteilung angehört.

Requests

Ein Request ist allgemein ein Antrag auf eine Änderung. Die Änderung kann unterschiedlicher Natur sein. Dies wird durch den Request-Modus festgelegt. Beispiele für Request-Modi sind etwa Änderung von Personendaten, Zuordnung oder Entfernung von Ressourcen, Anwendungsberechtigungen oder Active Directory-Gruppen. Ein Request wird immer von einer Person beantragt und kann sich auf die gleiche oder eine andere Person beziehen. Ein Request kann einem Genehmigungsworkflow unterliegen. Zur Ausführung eines Request kommt es erst, wenn der Genehmigungsworkflow erfolgreich beendet wurde (alle eingebundenen Stellen haben den Request genehmigt).

Genehmigungsworkflow

Genehmigungsworkflows steuern, ob ein Request tatsächlich zur Ausführung gelangt (ob die beantragte Änderung tatsächlich durchgeführt wird) oder nicht. Genehmigungsworkflows können aus unterschiedlichen Schritten bestehen, wobei der direkte Vorgesetzte (oder Abteilungsverantwortliche) als Vorgesetzter der Person, der etwas zugeordnet werden soll, als auch der Verantwortliche des Objekts (der Ressource, der Berechtigung, der Gruppe), welches zugeordnet werden soll eine spezielle Stellung einnehmen. Im Genehmigungsworkflow wird auf diese beiden Rollen lediglich abstrakt referenziert. Wird ein Request erstellt, so werden die betroffenen Personen eruiert und in den jeweiligen Request im Workflow als Genehmiger hinterlegt - sofern der Vorgesetzte und der Dateneigentümer im Workflow als entsprechende Schritte vorgesehen sind.

3.2 tenfold Komponenten

tenfold operiert durch das Zusammenspiel mehrerer Komponenten. Hierbei handelt es sich grob um:

- Die tenfold-Datenbank (Microsoft SQL Server oder Oracle Database)
- Den tenfold-Server Dienst
- Ein oder mehrere tenfold-Agents

3.2.1 tenfold Datenbank

In der Datenbank werden, neben den historischen Daten zu Personen und Berechtigungen, auch die große Mehrheit der Einstellungen von tenfold abgespeichert. Die tenfold Datenbank wird mit jedem Update von tenfold automatisch mitaktualisiert.

Datensicherung

Wenn Sie eine Datensicherung von tenfold vornehmen, achten Sie darauf, die Datenbank immer in die Sicherungen miteinzubeziehen.

Die Verbindungseinstellungen werden bei der Installation von tenfold eingerichtet (siehe [Installation](#)(see page 26)). Damit eine Verbindung zwischen dem tenfold-Server und der Datenbank hergestellt werden kann müssen daher auf der Firewall die entsprechenden Ports freigeschaltet werden. Standardmäßig sind dies folgende Ports:

DBMS	Port
Microsoft SQL Server	1433
Oracle Database	1521

Ports

Bei den oben genannten Ports handelt es sich lediglich um die normalerweise voreingestellten Ports der jeweiligen Datenbanksysteme. Diese können jedoch umkonfiguriert werden. Achten Sie daher darauf die korrekten Ports in der Firewall freizuschalten.

TCP

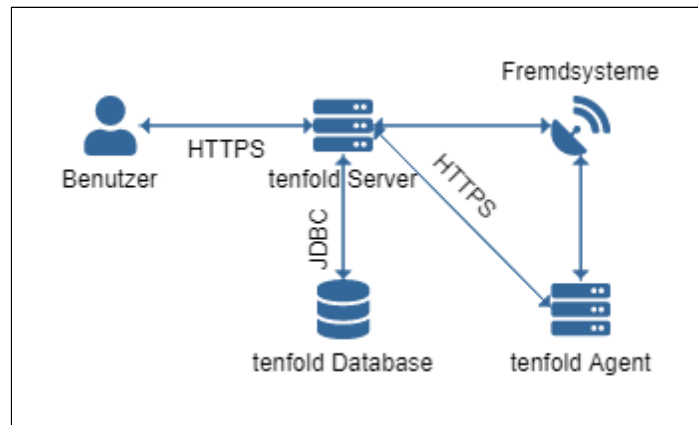
Es ist möglich Datenbanksysteme auch über andere Wege als TCP anzusprechen. Beispielsweise erlaubt es Microsoft SQL Server Verbindungen auch über Shared Memory aufzubauen. Beachten Sie, dass tenfold Verbindungen nur über TCP unterstützt. TCP-Verbindungen müssen daher auf Seiten der Datenbank aktiviert sein.

Nur der tenfold Server-Dienst bedient die Datenbank. Eine offene Verbindungsmöglichkeit zwischen tenfold Agenten und der Datenbank ist **nicht** erforderlich.

3.2.2 tenfold Server

Der tenfold-Server-Dienst ist der Prozess, welcher den HTTP-Server für die Benutzerschnittstelle aufbaut und die Datenbank bedient. Anwender bedienen tenfold ausschließlich über diese Schnittstelle. Auf Seiten der Anwender ist keinerlei weitere Freischaltung notwendig; alle Operationen werden mit entsprechenden Dienstkonten, welche in tenfold hinterlegt sind, durchgeführt. Es ist daher zum Beispiel nicht notwendig, dass

der Anwender entsprechende Berechtigungen im Active Directory hat, um mittels tenfold Operationen im Active Directory durchzuführen. Lediglich die entsprechenden Berechtigungen in tenfold müssen vorhanden sein.



Für den Zugriff auf die Web-Oberfläche wird normalerweise HTTPS verwendet, welches standardmäßig den Port 443 verwendet. Sollte tenfold diesen Port nicht verwenden können, da er bereits belegt ist, ist die Verwendung des Ports 8443 nicht unüblich. Stellen Sie sicher, dass der entsprechende Port auf der Firewall freigegeben ist.

Neben der Datenbank benötigt der tenfold Server-Dienst auch noch Zugriff auf das Active Directory. Dieser Zugriff findet über das LDAP(S)-Protokoll statt. Die Standard-Ports dafür sind 389 (unverschlüsselt) und 636 (verschlüsselt).

Unverschlüsselte LDAP-Verbindung

Obwohl eine verschlüsselte Verbindung explizit nur für das Setzen von Kennwörtern zwingend erforderlich ist, verwendet tenfold ausschließlich verschlüsselte Verbindungen für die Kommunikation mit Active Directory.

Für den Zugriff auf Dateien (zum Beispiel CSV-Importe) kann es notwendig sein, dass der Benutzer, unter welchem der tenfold Server-Dienst läuft, Zugriff auf entsprechende Verzeichnisse benötigt.

Dateifreigabe

Da tenfold in vielen Fällen unter dem lokalen System-Konto läuft ist es zu empfehlen, für den Austausch von Import-Dateien eine Dateifreigabe auf der Maschine einzurichten, auf welcher der tenfold Server-Dienst läuft. Daraufhin können die anderen Systeme ihre Dateieporte einfach auf die Dateifreigabe von tenfold schreiben.

3.2.3 tenfold Agents

Bei den Agenten handelt es sich um Dienste, welche auf derselben Maschine wie tenfold laufen können oder auch auf entfernten Maschinen. Der tenfold-Server kontaktiert die Agenten bei Bedarf, um Tätigkeiten im Microsoft-Umfeld durchzuführen. Dazu gehören:

- Fileserver-Operationen (Anlage von Verzeichnissen, Vergabe von Berechtigungen, etc.)
- Exchange-Operationen (Anlage von Mailboxen, Auslesen der Berechtigungen, etc.)
- Sharepoint-Operationen (Auslesen der Berechtigungen, etc.)
- Microsoft 365-Operationen (Vergabe von Berechtigungen, etc.)

Nur das Active Directory selbst wird direkt vom tenfold Server-Dienst über das LDAP-Protokoll angesteuert. Für Fileserver-Berechtigungen verwendet der Agent Standard-NTFS-Befehle über das CIFS/SMB-Protokoll. Für die meisten anderen Systeme kommuniziert der Agent mit dem System mittels Powershell und/oder Webservices, welche von Microsoft zur Verfügung gestellt werden. Oftmals ist es daher nicht nur notwendig, die entsprechenden Netzwerk-Ports auf der Firewall freizuschalten, sondern auch das Powershell-Remoting zu aktivieren.

Powershell-Plugin

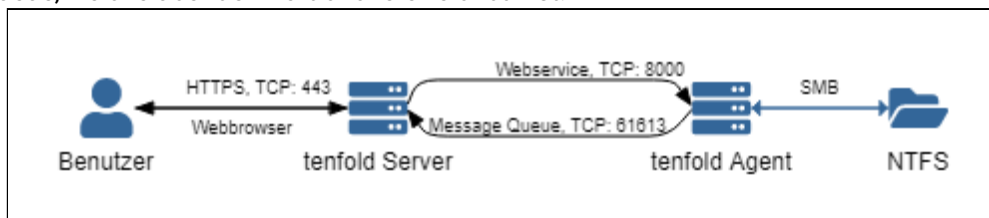
Zusätzlich zu den Standard-Funktionen verwendet auch das Powershell-Plugin den tenfold Agenten, um Benutzerdefinierte Powershell-Skripte durchzuführen.

Da der Agent die Fileserver-Operationen mit dem Account durchführt, unter welchem auch der Dienst läuft (wird bei der Installation des Agenten festgelegt), muss der Account auch über entsprechende Berechtigungen auf den betroffenen Fileshares verfügen. Dies bedeutet im Normalfall "Vollzugriff", da nur damit auch Berechtigungen vergeben werden können.

SMB Ports

Normalerweise werden die Ports für Fileserver-Zugriffe nicht von Firewalls blockiert. Sollte die Verbindung zum Fileserver nicht aufgebaut werden können, prüfen Sie ob die Ports 139 und 445 blockiert werden.

Der Agent selbst horcht standardmäßig auf dem Port 8000. Sollte dieser auf einer anderen Maschine als der tenfold Server-Dienst installiert sein, so muss die Kommunikation über diesen Port gewährleistet sein. Für länger andauernde Scan-Operationen verwenden der tenfold Server-Dienst und die tenfold Agenten eine Message-Queue, welche über den Port 61613 erreichbar ist.



Mehrere tenfold Server für einen Agenten

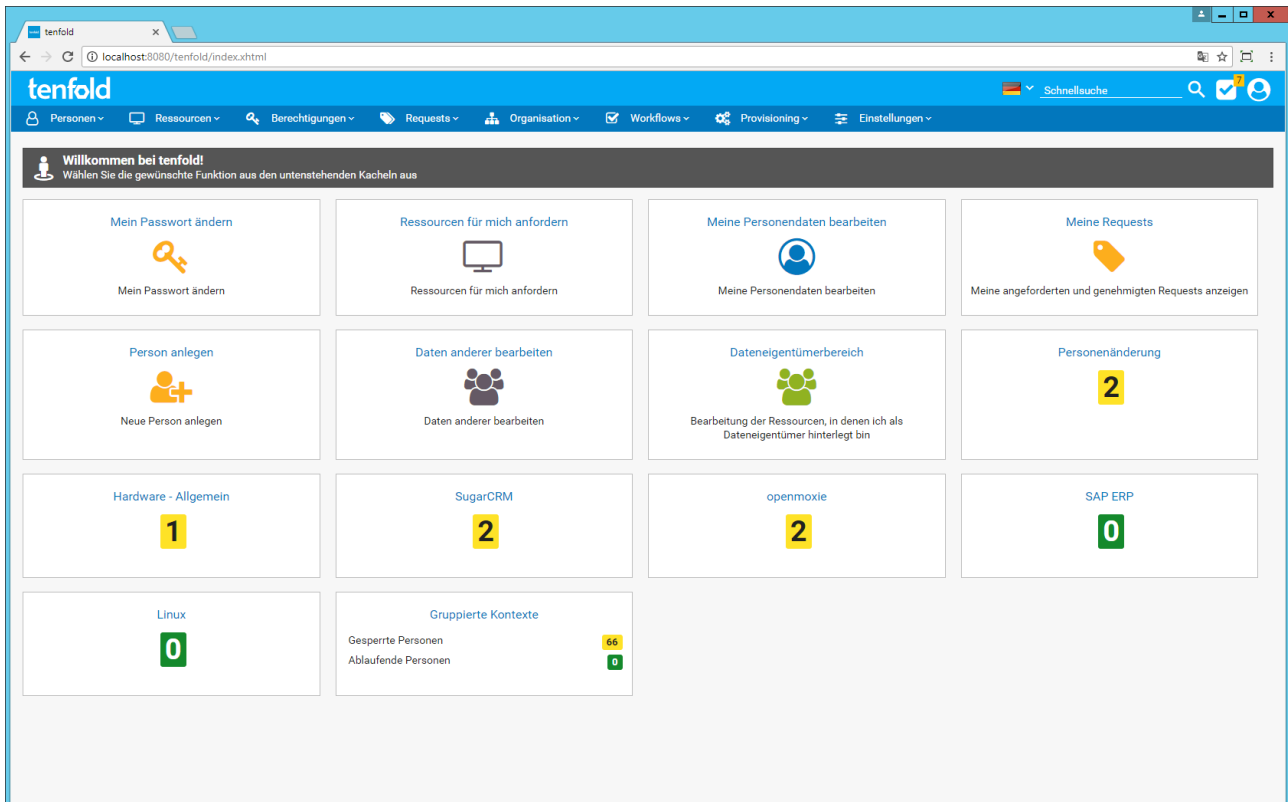
Agenten sind eigenständige Prozesse, welche unabhängig von einem bestimmten tenfold Server-Dienst laufen. Da der Server-Dienst und der Agent jedoch Zertifikate austauschen wird dabei der Agent an den Server gebunden. Ab diesem Zeitpunkt akzeptiert der Agent keine Anfragen von anderen Servern mehr.

3.3 Self-Service-Oberfläche

Neben den Administrationsmasken, welche vorwiegend für geschultes IT-Personal bestimmt sind, verfügt tenfold über eine Oberfläche, die für die Bedienung durch den Endanwender geeignet ist. Diese Oberfläche bekommt der Anwender beim Start der Anwendung zu sehen. Für die Bedienung ist das Anwendungsmenü nicht erforderlich.

Berechtigungen und Konfiguration

Wie häufig ist die Darstellung der Oberfläche von mehreren Einstellungen und von den zugeordneten Berechtigungen des gerade angemeldeten Benutzers abhängig. Es ist daher möglich, dass Ihre konkrete Oberfläche von der Beschreibung in bestimmten Punkten abweicht. Dies kann daran liegen, dass die Konfiguration des Systems abweichend festgelegt wurde, oder Sie nicht über die notwendigen Berechtigungen verfügen, um alle beschriebenen Funktionen zu nutzen.



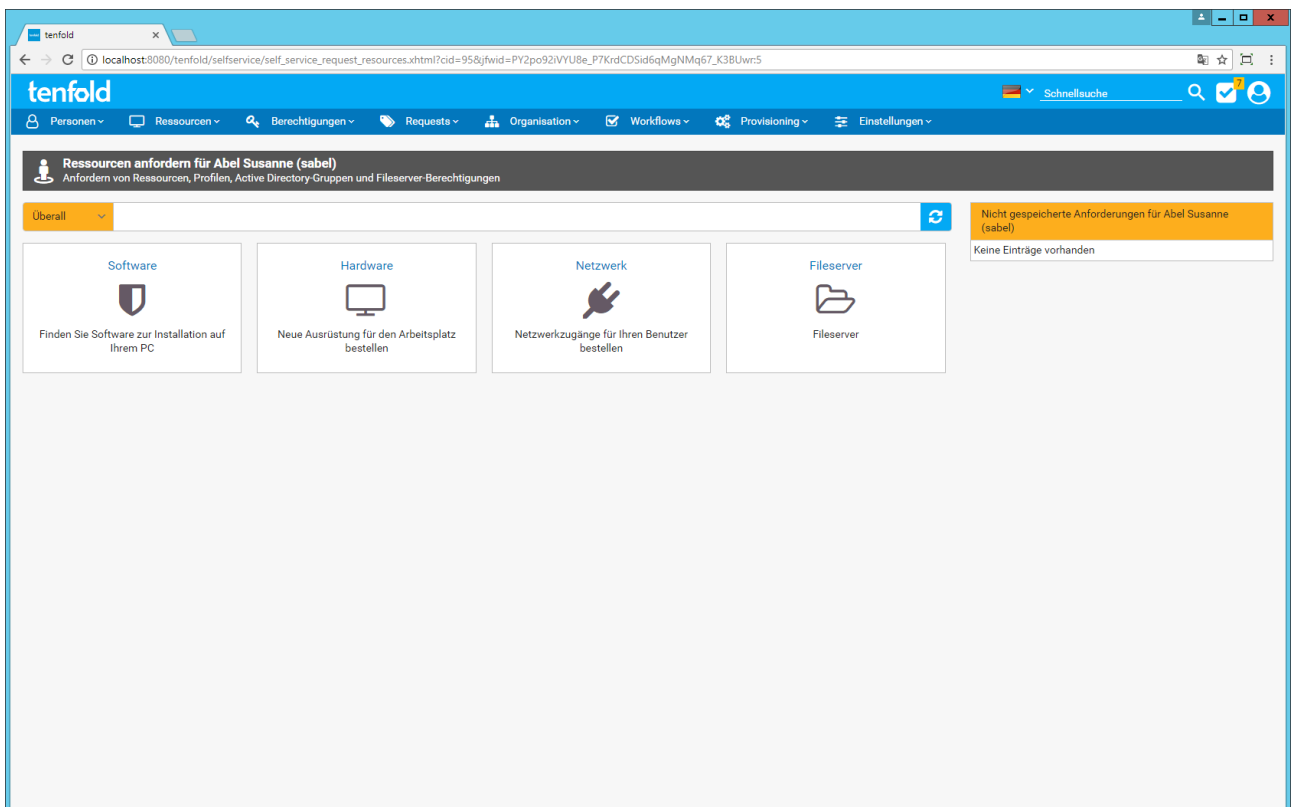
Über die Self-Service-Oberfläche können die nachfolgend im Detail beschriebenen Tätigkeiten durchgeführt werden.

3.3.1 Passwortänderung

3.3.2 Ressourcenanforderung

Allgemeines

Diese Funktion steht über die Kachel "Ressourcen für mich anfordern" für die eigene Person zur Verfügung. Um eine Ressourcenanforderung für eine andere Person zu starten, ist die Kachel "Für andere anfordern" und nach der Personenauswahl die Kachel "Ressourcen anfordern" zu wählen. Jede Anfrage wird in einem Warenkorb (siehe "Nicht gespeicherte Anforderungen für") vermerkt. Erst durch das abschließende Speichern werden die Requests tatsächlich in der Datenbank angelegt. Der Warenkorb existiert für jede Person, für die Ressourcen angefordert wurden separat.

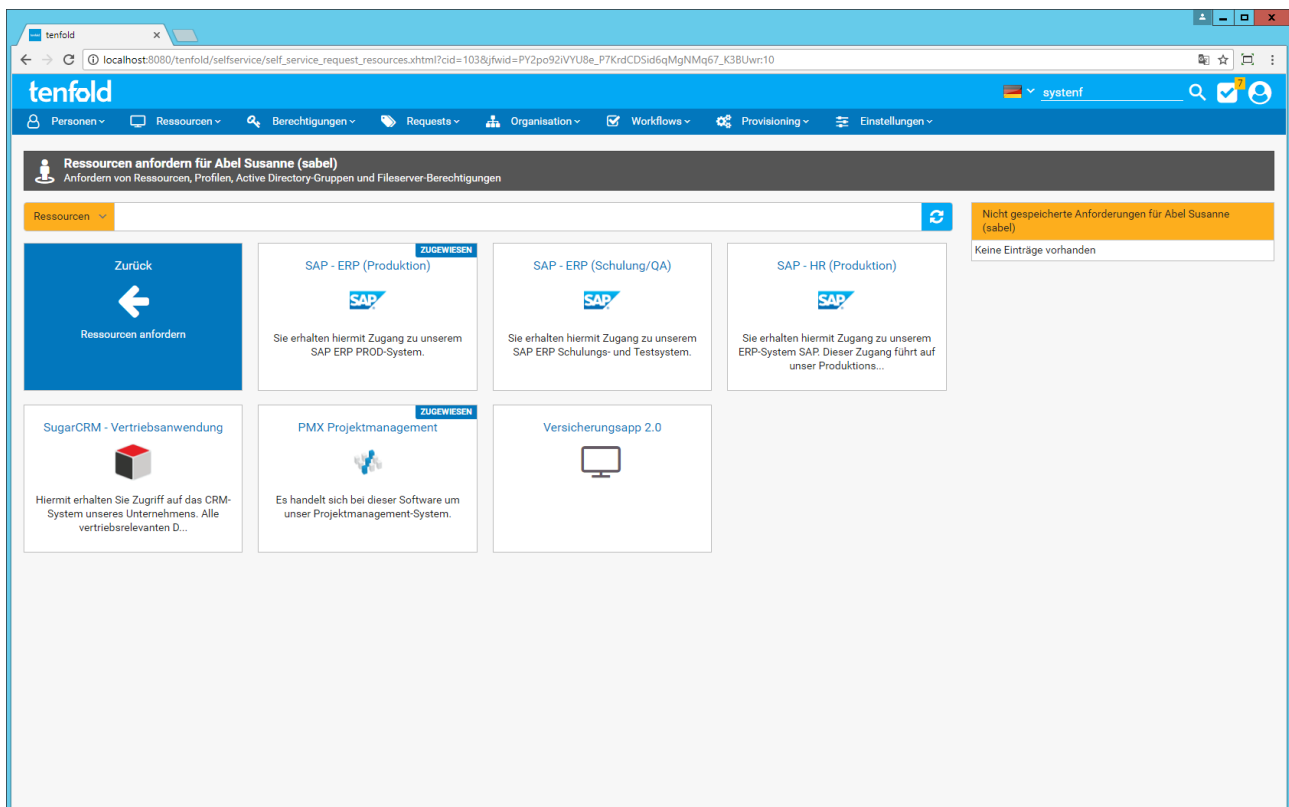


Diese Funktion erlaubt es, dass in tenfold konfigurierte IT-Ressourcen für einen Anwender angefordert werden können. Diese Ressourcen können unterschiedlich sein:

- Anwendungen und deren Berechtigungen (z.B. Rollen in einem ERP-System)
- Berechtigungen für Ordner auf Fileservern
- IT-Hardware (PCs, Laptops, Telefone)
- IT-Funktionen (VPN-Zugang, Social-Media-Freigabe)

Ressourcenauswahl

Auf der Auswahlmaske stehen nun die unterschiedlichen in tenfold konfigurierten Ressourcenkategorien, sowie die Sonderkategorien "Fileserver", "Active Directory-Gruppen" und "Profile" zur Verfügung. Durch Klick auf eine der Kategorien, gelangt man zu den Ressourcen dieser Kategorie.



Wenn Sie nicht sicher sind, in welcher Kategorie sich die gewünschte Ressource befindet, können Sie auch das Suchfeld über den Kacheln benutzen um Ressourcen mit dem gewünschten Namen zu finden.

Suchen in der Beschreibung

Wenn die Systemeinstellung "Self-service > Beschreibung durchsuchen" aktiviert ist, wird mit dem Suchfeld auch die Beschreibung der Ressourcen nach den eingegebenen Suchbegriffen durchsucht.

Durch einen Klick auf die gewünschte Ressource wird der Anforderungsprozess gestartet.

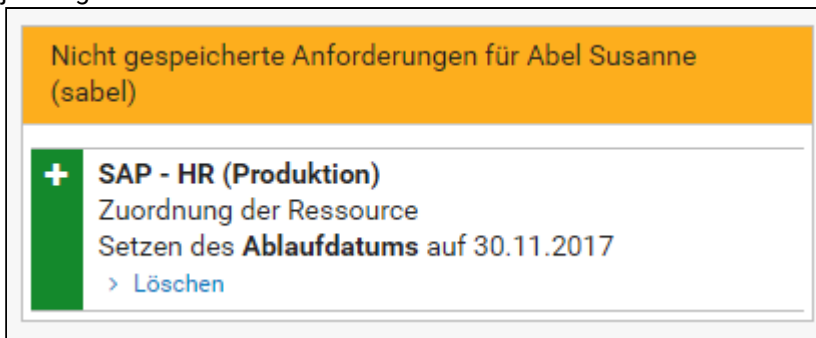
Festlegung von Optionen und Berechtigungen

Je nach Konfiguration erfolgt nunmehr die Eingabe einer Bemerkung, eines gewünschten Ablaufdatums, die Festlegung von Optionen und die Auswahl von Berechtigungen (im Falle, dass es sich bei der gewünschten Ressource um einen Zugang zu einer Anwendung handelt, wird über die Berechtigungszuordnung festgelegt, welche Berechtigungen der Benutzer in der Anwendung haben soll). Je nach Konfiguration sind diese Angaben optional oder verpflichtend.

Mehrfache Zuordnungen

Bereits dem ausgewählten Benutzer zugeordnete Ressourcen werden mit dem Zusatzhinweis "Zugewiesen" markiert. Je nach Einstellungen der Ressource ist es möglich, die gleiche Ressource mehrmals oder nur einmalig zugeordnet zu haben. Klickt man auf eine bereits zugeordnete Ressource, erscheint dementsprechend gegebenenfalls ein Hinweis, dass die Ressource nur einmalig zugeordnet werden kann.

Durch Klick auf den Button "Anfordern" landet die Anforderung im Warenkorb (rechte Bildschirmseite) für den jeweiligen Benutzer.



Über den Link "Löschen" kann ein Eintrag wieder aus dem Warenkorb entfernt werden.

Bestehende Zuordnung bearbeiten

Soll keine neue Ressource angefordert werden, sondern lediglich eine bestehende Zuordnung bearbeitet werden (zum Beispiel Änderung von Optionen oder des Ablaufdatums oder Setzen bzw. Löschen bestimmter Berechtigungen in einer Anwendung), so muss die entsprechende Ressource ausgewählt werden (in diesem Fall muss die Kennzeichnung "Zugeordnet" vorliegen). Anschließend ist die Kachel "Bestehende Zuordnung bearbeiten" auszuwählen.

Anschließend kann die Zuordnung auf die gleiche Weise bearbeitet werden, wie dies bei einer neuen Anforderung der Fall ist. Der Request, der hieraus generiert wird, hat die gewünschte Datenänderung zum Inhalt.

Mehrfache Zuordnung

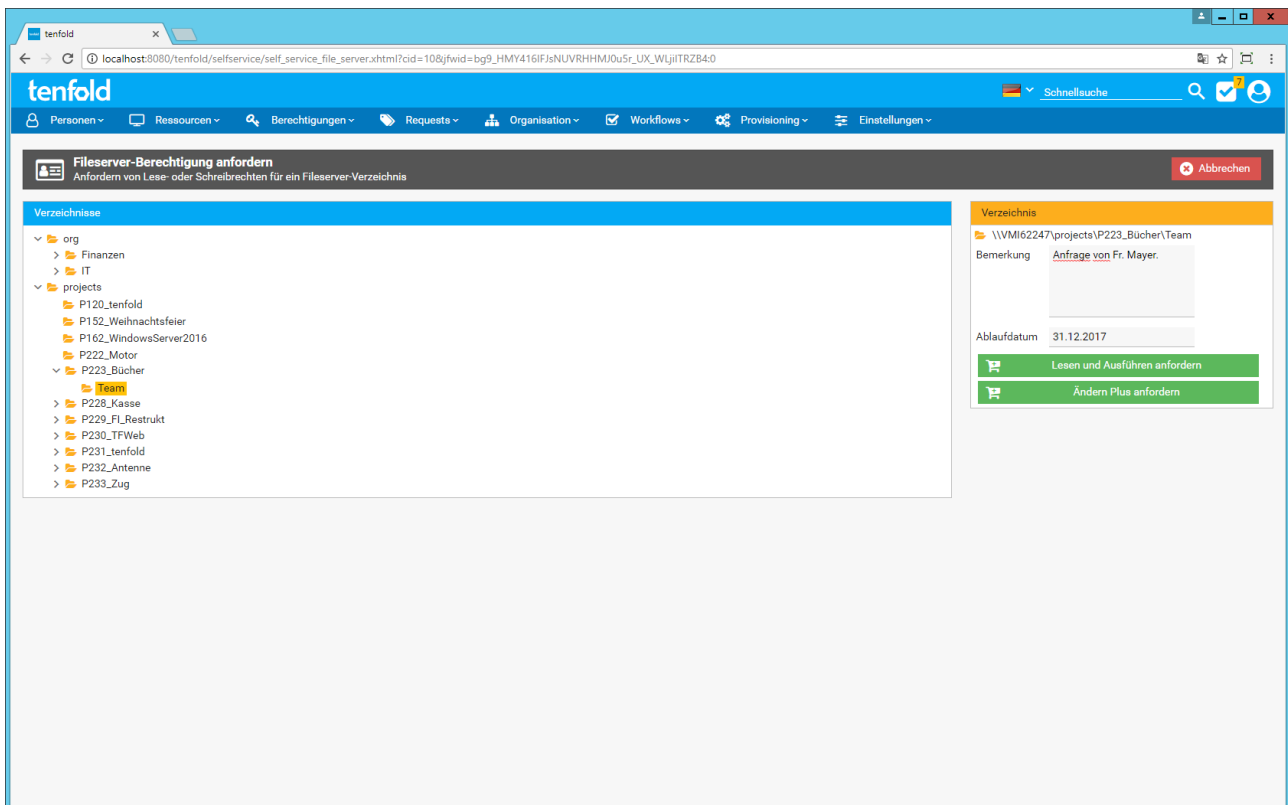
Sind mehrfache Zuordnungen der gleichen Ressource möglich, so muss der entsprechend zutreffende Eintrag, der bearbeitet werden soll, ausgewählt werden.

Bestehende Zuordnung löschen

Löschen

Das Löschen von bestehenden Ressourcenzuordnungen über die Self-Service-Oberfläche wird aktuell noch nicht unterstützt. Hierzu ist ein Eingriff durch den IT-Administrator erforderlich.

Spezialkategorie Fileserver



Für Berechtigungen auf Ordner auf Fileservern existiert - konfigurationsabhängig - die Spezialkategorie Fileserver, deren Maskenaufbau aufgrund der Datenstruktur von den restlichen Kategorien abweicht. Auf der Maske für die Anforderung von Fileserver-Berechtigungen befindet sich auf der linken Seite ein Baum von Verzeichnissen. Die Verzeichnisse, die hierbei zur Auswahl stehen, sind - je nach Konfiguration - gegebenenfalls nicht alle Verzeichnisse, die auf dem Fileserver zur Verfügung stehen, sondern nur bestimmte, zur Anforderung freigegebene Verzeichnisse. (entweder generell alle Verzeichnisse des Fileservers - somit keine Einschränkung, nur alle Verzeichnisse bis zu einer bestimmten Verzeichnisebene oder nur diejenigen Verzeichnisse, die durch den Administrator explizit freigegeben wurden).

Um eine Anforderung für Berechtigungen für einen bestimmten Ordner zu stellen, gehen Sie folgendermaßen vor:

1. Wählen Sie den gewünschten Ordner im Verzeichnisbaum auf der linken Seite aus.
2. Geben Sie bei Bedarf eine Bemerkung in das Textfeld ein (diese Bemerkung können die Entscheider im Genehmigungsworkflow sehen)
3. Geben Sie ein Ablaufdatum ein, sofern die Berechtigung automatisch zu einem bestimmten Zeitpunkt entzogen werden soll
4. Klicken Sie anschließend auf den Anforderungs-Button, der der gewünschten Berechtigungsstufe entspricht
5. Anschließend landet der Request im Warenkorb.

Im Normalfall bestehen die verfügbaren Berechtigungsstufen aus "Lesen & Ausführen" (wenn nur lesender Zugriff benötigt wird) und "Ändern" bzw. "Ändern Plus" (wenn Daten nicht nur gelesen, sondern auch bearbeitet werden können sollen).

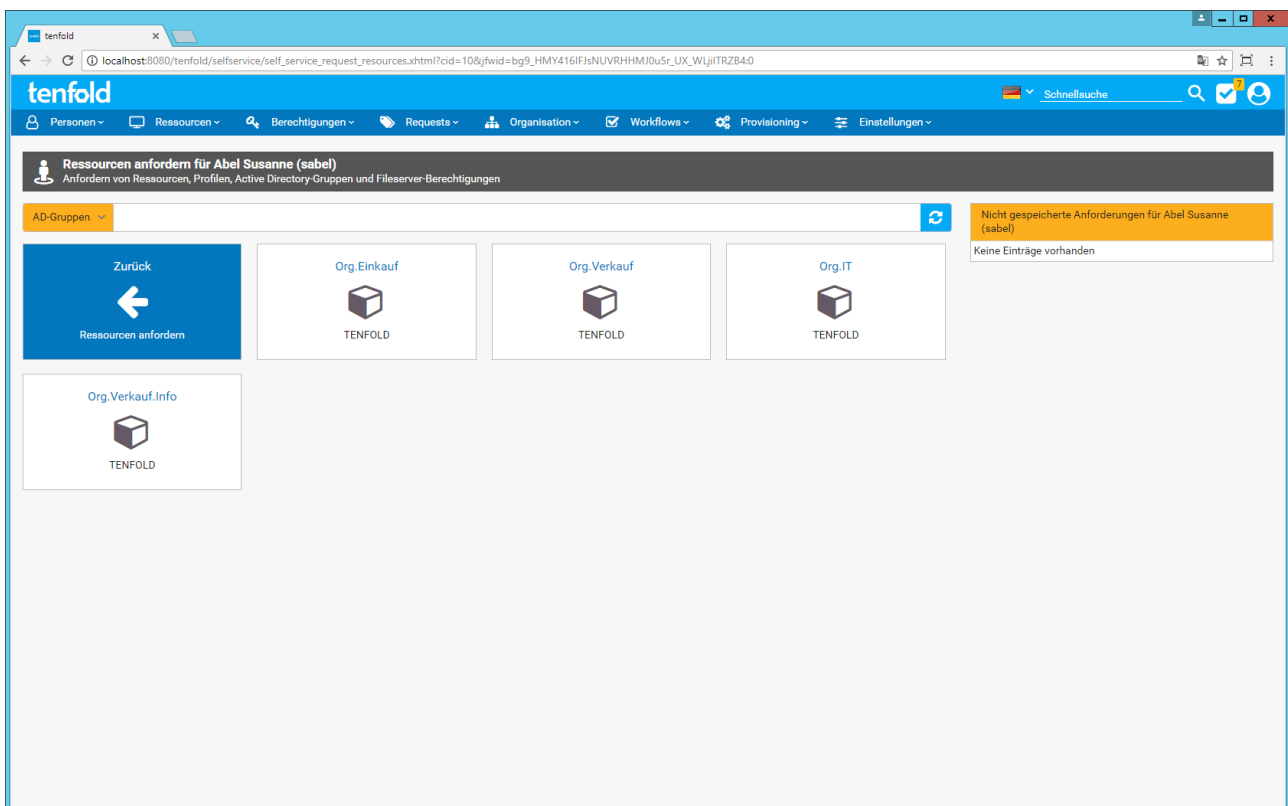
Die Anforderung für das Löschen von bestehenden Fileserver-Berechtigungen ist über die Self-Service-Oberfläche nicht möglich.

Unterverzeichnisse und bestehende Berechtigungen

Wenn Sie ein Verzeichnis auswählen und auf der rechten Seite im Bereich "Verzeichnis" nur der Verzeichnisname aufscheint (ohne Anforderungs-Buttons), dann ist dieses Verzeichnis nicht für Anforderungen freigegeben. Es wird lediglich der Vollständigkeit des Pfades halber dargestellt, da die Anforderung für eines der Unterverzeichnisse möglich ist.

Wenn der gewünschte Benutzer auf das gewünschte Verzeichnis bereits Berechtigungen hat, so wird dies durch einen entsprechenden Warnhinweis gekennzeichnet.

Spezialkategorie Active Directory-Gruppen



Für die explizite Anforderung einer Gruppenmitgliedschaft steht die Spezialkategorie "Active Directory-Gruppen" zu Verfügung. Innerhalb der Kategorie werden alle Active Directory-Gruppen, welche für Self-Service-Anforderungen zur Verfügung stehen, als Kacheln dargestellt. Die Überschrift zeigt dabei den Anzeigenamen der Gruppe an und der Untertitel gibt die Domäne an, in welcher die Gruppe existiert. Zur Auswahl stehen nicht alle Gruppen im Active Directory, sondern nur diejenigen, welche explizit für Self-Service freigeschaltet wurden.

Um eine Anforderung für eine Mitgliedschaft in einer bestimmten Gruppe zu stellen, gehen Sie folgendermaßen vor:

1. Wählen Sie die gewünschte Gruppe aus, indem Sie auf die jeweilige Kachel klicken
2. Geben Sie bei Bedarf eine Bemerkung in das Textfeld ein (diese Bemerkung können die Entscheider im Genehmigungsworkflow sehen)

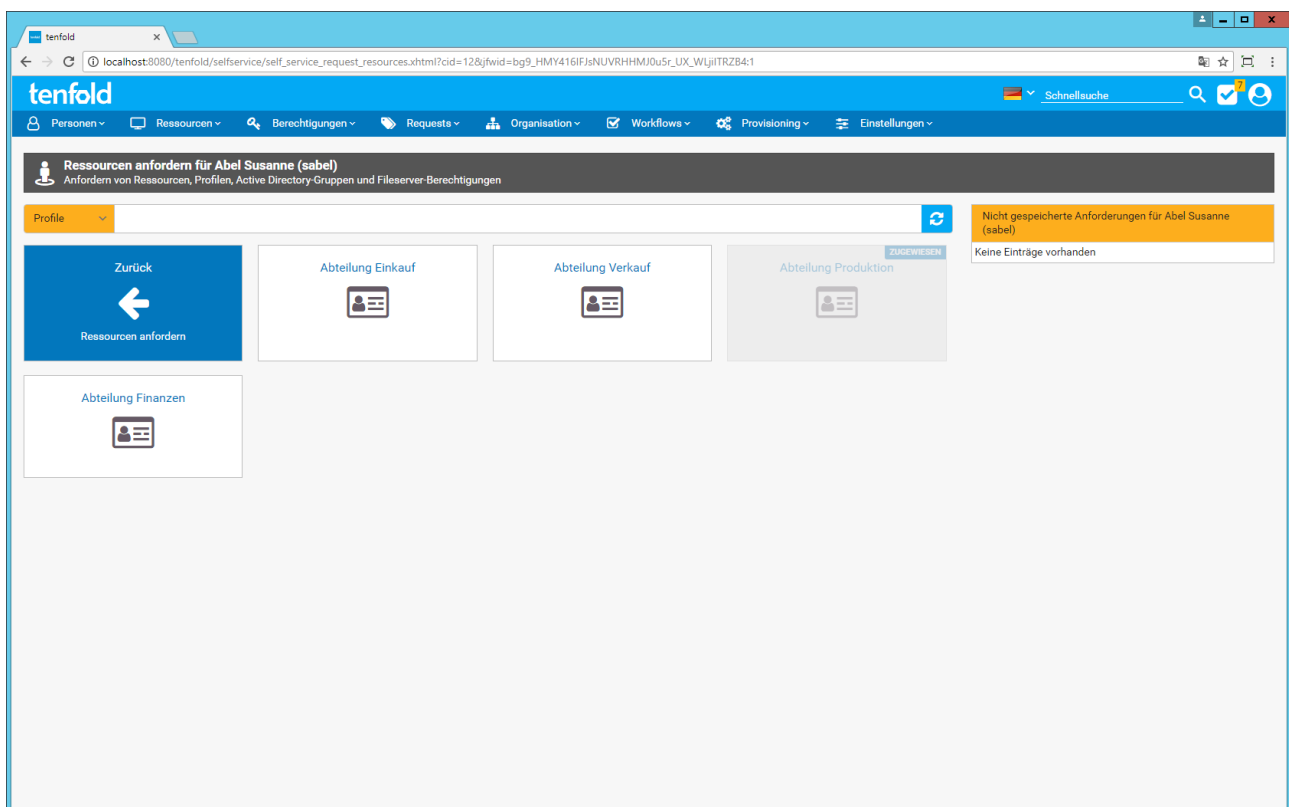
3. Geben Sie ein Ablaufdatum ein, sofern die Mitgliedschaft automatisch zu einem bestimmten Zeitpunkt beendet werden soll
4. Klicken Sie anschließend auf den Anfordern-Button.
5. Anschließend landet der Request im Warenkorb.

Einschränkungen

Es ist nicht möglich, die Mitgliedschaft in Fileserver-Berechtigungsgruppen über die Funktion anzufordern. Die Mitgliedschaft in Fileserver-Berechtigungsgruppen wird immer implizit über Auswahl von Verzeichnis und Berechtigungsstufe verwaltet. Eine explizite Verwaltung dieser Gruppen über tenfold ist nicht möglich.

Das Beenden von bestehenden Gruppenmitgliedschaften über die Self-Service-Oberfläche wird aktuell noch nicht unterstützt. Hierzu ist ein Eingriff durch den IT-Administrator erforderlich.

Spezialkategorie Profile



In der Spezialkategorie "Profile" können Profile (vordefinierte Sets an Berechtigungen aus mitunter unterschiedlichen Systemen) implizit angefordert werden. Ein Profil dient der Gruppierung von unterschiedlichen Berechtigungen in einem Warenkorb, um diese dann gesammelt und automatisiert durch das System anzufordern. Wird einer Person ein Profil zugeordnet (und wird diese Zuordnung durch den Genehmigungsworkflow freigegeben), so stellt tenfold automatisch alle Requests, die notwendig sind, um die im Profil definierten Ressourcen der Person zuzuordnen.

Automatische Zuordnungen

Je nach Konfiguration werden den Personen bereits systemseitig aufgrund von definierten Regeln bestimmte Profile automatisch zugewiesen. Diese Einstellungen werden durch den Administrator festgelegt.

Um eine Anforderung für eine Mitgliedschaft in einer bestimmten Gruppe zu stellen, gehen Sie folgendermaßen vor:

1. Wählen Sie das gewünschte Profil aus, indem Sie auf die jeweilige Kachel klicken
2. In der Folge wird angezeigt, welche Ressourcen durch die Zuordnung des Profils automatisch angefordert werden.
3. Geben Sie bei Bedarf eine Bemerkung in das Textfeld ein (diese Bemerkung können die Entscheider im Genehmigungsworkflow sehen)
4. Geben Sie ein Ablaufdatum ein, sofern die Mitgliedschaft automatisch zu einem bestimmten Zeitpunkt beendet werden soll
5. Klicken Sie anschließend auf den Anfordern-Button.
6. Anschließend landet der Request im Warenkorb.

tenfold | Schnellauche

Profilzuordnung anfordern
Anfordern einer Profilzuordnung

Abteilung Verkauf

Active Directory-Gruppen

Name

Org. Verkauf

Ressourcen

Name	Berechtigungen	Optionen	Informationen
PMX Projektmanagement	Vertrieb/Angabote, Vertrieb/Import, Vertrieb/CRM		
SugarCRM - Vertriebsanwendung	Administrator		
SAP - ERP (Produktion)	VK_ANGBT_01, VK_ANGBT_02, VK_AUFT, VK_PREISE, ALLG_BASIS		

Bemerkung

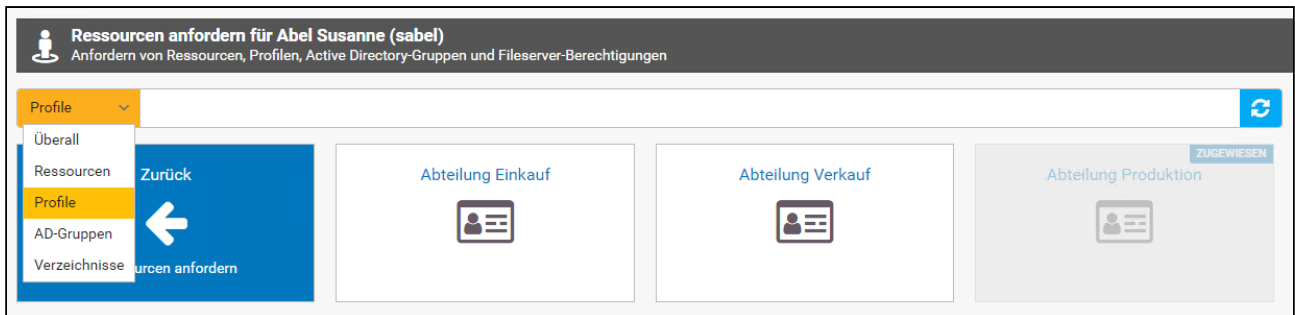
Ablaufdatum

Anfordern

Einschränkung

Das Beenden von bestehenden Profilzuordnungen über die Self-Service-Oberfläche wird aktuell noch nicht unterstützt. Hierzu ist ein Eingriff durch den IT-Administrator erforderlich.

Ressourcensuche



Wenn Sie nicht genau wissen, wo sich eine Ressource befindet, so können Sie die Suche nutzen. Diese befindet sich direkt unter der Toolbar, sofern Sie sich in einer der Ressourcenkategorien befinden. Die Suche wird ausgeblendet, wenn Sie eine Ressource ausgewählt haben und sich auf der Maske zur Festlegung der Optionen befinden. Im Suchfeld können Sie ein Textfragment der gesuchten Ressource eingeben. Über die Auswahlliste am linken Rand des Suchfelds können Sie einschränken, in welcher Kategorie Sie die Suche durchführen möchten. Wählen Sie den Eintrag "Überall", um in allen Kategorien zu suchen.

Beachten Sie, dass die Suche, je nach Anzahl der hinterlegten Ressourcen, Gruppen, Verzeichnisse und Profile einige Sekunden Zeit in Anspruch nehmen kann. Beachten Sie außerdem, dass die Suche aufgrund der notwendigen Performance nur für Verzeichnisse durchgeführt wird, welche explizit für Self-Service freigegeben sind, unabhängig davon, ob in der Fileserver-Konfiguration die Einstellung "Alle Verzeichnisse" oder "Bis Verzeichnisebene X" aktiviert wurde

3.3.3 Person anlegen und Personendatenänderung

Über die Kachel "Person anlegen" gelangen Sie zur Funktion für die Anlage einer neuen, aktuell noch nicht verwalteten Person. Für eine detaillierte Beschreibung der Funktionalität siehe auch [Personen](#) (see page 63). Die Funktion ist auch über das Menü Personen > Person anlegen verfügbar.

Über die Kachel "Datenänderung" gelangen Sie zur Bearbeitung der Stammdaten der jeweiligen Person. Für eine detaillierte Beschreibung der Funktionalität siehe auch [Personen](#) (see page 63). Diese Funktion steht über die Kachel "Meine Personendaten bearbeiten" für die eigene Person zur Verfügung. Um eine Datenänderung für eine andere Person zu starten, ist die Kachel "Daten anderer bearbeiten" und nach der Personenauswahl die Kachel "Personendaten bearbeiten" zu wählen.

3.3.4 Meine Requests

Objekt	Beschreibung	Angefordert am	Request-Typ	Request-Status
P233_Zug	Verzeichnis von P233_Zug umbenennen auf P233_Zugfahrer	30.10.2017 18:11:31	Änderung	GERPLANT
VPN-Zugang	Ressourcenzuordnung löschen: VPN-Zugang	25.10.2017 15:26:04	Löschen	FERTIG
SugarCRM - Vertriebsanwendung	Ressourcenzuordnung löschen: SugarCRM - Vertriebsanwendung	25.10.2017 15:26:04	Löschen	FERTIG
PMX Projektmanagement	Ressourcenzuordnung löschen: PMX Projektmanagement	25.10.2017 15:26:04	Löschen	FERTIG
Desktop PC	Ressourcenzuordnung löschen: Desktop PC	25.10.2017 15:26:04	Löschen	FERTIG
Person masterdata change	Person löschen	25.10.2017 15:26:02	Löschen	FERTIG
Team	Neue Berechtigung Ändern Plus für Benutzer ffaber auf Verzeichnis Team	25.10.2017 15:18:16	Änderung	FERTIG
Austausch	Neue Berechtigung Lesen und Ausführen für Benutzer Org.Einkauf auf Verzeichnis Austausch Neue Berechtigung Lesen und Ausführen für Benutzer Org.Finzen auf Verzeichnis Austausch Neue Berechtigung Lesen und Ausführen für Benutzer Org.Verkauf auf Verzeichnis Austausch Neue Berechtigung Lesen und Ausführen für Benutzer Org.Produktion auf Verzeichnis Austausch	25.10.2017 15:14:31	Änderung	FERTIG
Org.Einkauf	ffaber hinzufügen zu Org.Einkauf	25.10.2017 15:03:20	Änderung	FERTIG
SAP - ERP (Produktion)	Gewährte Anwendungsberechtigungen: PP_PROD_VIEW	25.10.2017 15:03:20	Änderung	FERTIG
Org.Finzen	ffaber entfernen von Org.Finzen	25.10.2017 14:54:22	Änderung	FERTIG
SAP - ERP (Produktion)	Entzogene Anwendungsberechtigungen: FNZ_BASIS, FNZ_JAB	25.10.2017 14:54:22	Änderung	FERTIG
Org.Verkauf	ffaber hinzufügen zu Org.Verkauf	25.10.2017 14:54:09	Änderung	FERTIG
PMX Projektmanagement	Gewährte Anwendungsberechtigungen: Vertrieb/CRM, Vertrieb/Angebote, Vertrieb/Import	25.10.2017 14:54:09	Änderung	FERTIG
SugarCRM - Vertriebsanwendung	Gewährte Anwendungsberechtigungen: Administrator	25.10.2017 14:54:09	Änderung	FERTIG
SAP - ERP (Produktion)	Gewährte Anwendungsberechtigungen: VK_ANGBT_01, VK_ANGBT_02, VK_AUFT, VK_PREISE	25.10.2017 14:54:09	Änderung	FERTIG

Die Funktion bietet eine Listenansicht über alle Requests, die entweder vom aktuellen Benutzer gestellt wurde, oder in denen der aktuelle Benutzer als Genehmiger aktiv war. Zur Liste gelangt man über einen Klick auf die Kachel "Meine Requests".

Filter

Über die Einstellungen im Bereich "Filter" kann die Anzeige beeinflusst werden:

- Datum: Es kann entweder ein vordefinierter Bereich, zum Beispiel "in den letzten 30 Tagen" gewählt werden, oder ein spezifischer Bereich mit Von- und Bis-Datum eingegeben werden. Dazu muss die Einstellung "spezielles Datum" gewählt werden
- Filter: Es können alle Requests, wo der Benutzer Antragsteller oder Genehmiger war angezeigt werden, oder auf eine von beiden Sachverhalten eingeschränkt werden.

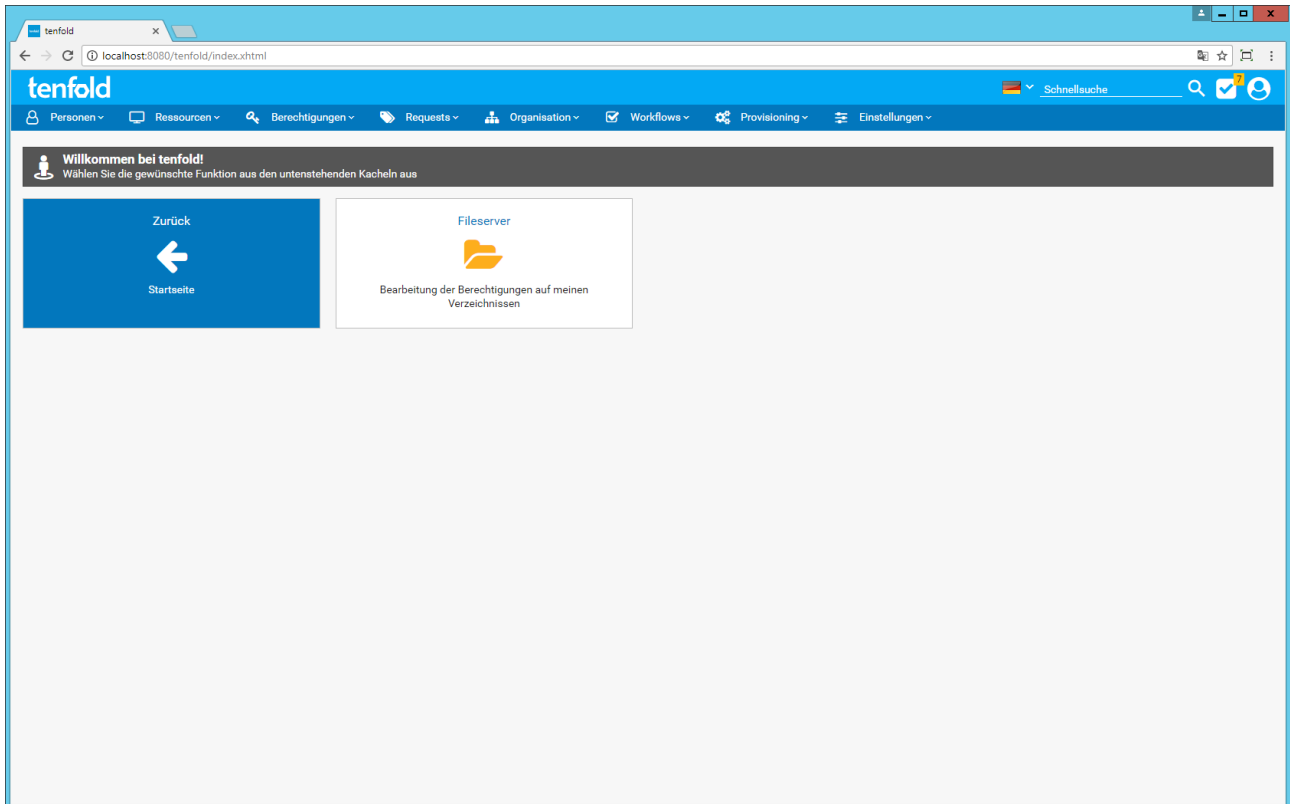
Anzeige und Aktionen

Folgende Spalten zeigen nähere Informationen zum Request an:

- Objekt: welches Objekt vom Request betroffen war. Das Icon deutet dabei den jeweiligen Request-Modus an.
- Beschreibung: eine kurze Zusammenfassung des Requestinhalts
- Angefordert am: Das Datum, an welchem der Request in der Datenbank gespeichert wurde
- Request-Typ: Zeigt den Typ des Request an
- Status: Zeigt an, in welchem Status sich der Request aktuell befindet

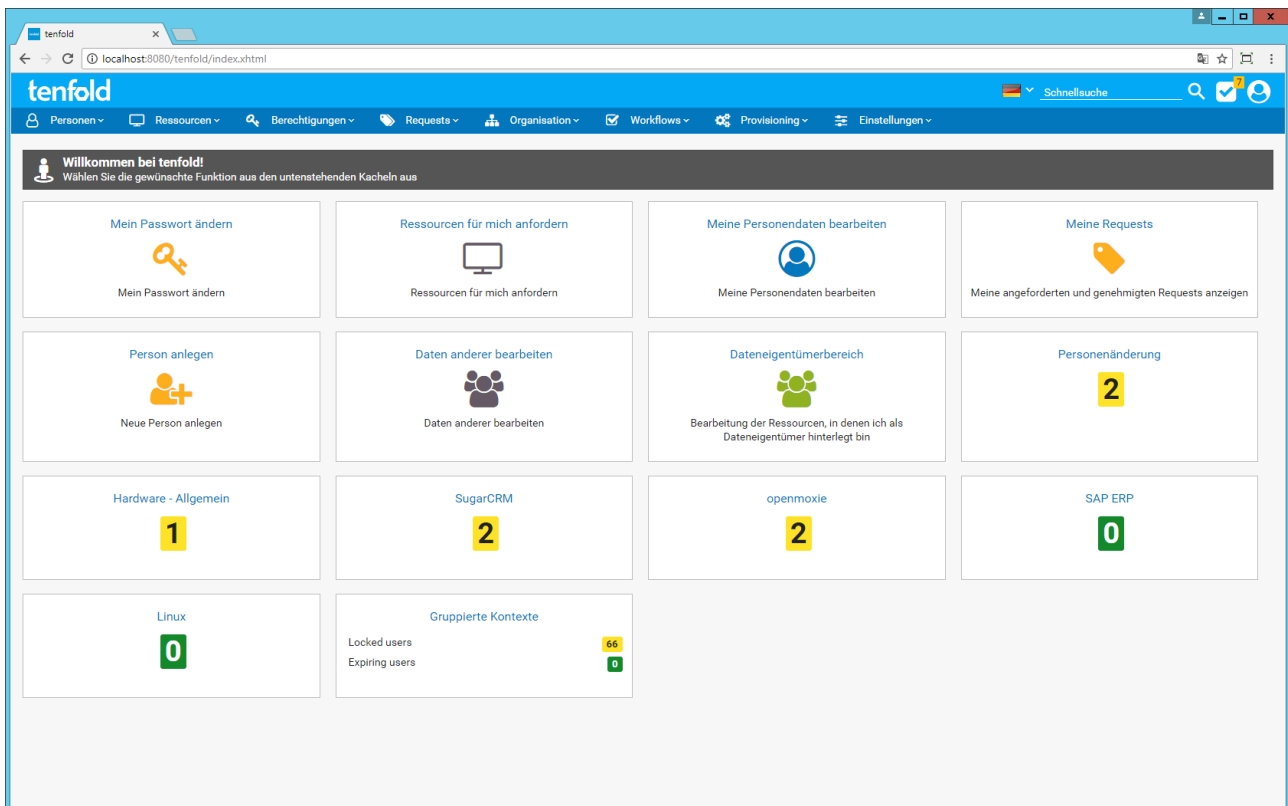
Über das Kontextmenü in der jeweiligen Zeile kann auf die Maske "Request anzeigen" und "Person anzeigen" (entspricht dem Empfänger / "Angefordert für" aus dem Request) verzweigt werden. Für eine detaillierte Beschreibung der Maske "Request anzeigen" siehe auch [Requests](#)(see page 352).

3.3.5 Dateneigentümerbereich



Der Dateneigentümerbereich dient dazu, dem Dateneigentümer von Ressourcen die Möglichkeit zu bieten, eine Zusammenfassung aller ihm zugeordneten Ressourcen zu zeigen, und dann in die jeweilige Verwaltung der entsprechenden Ressourcen zu verzweigen. Diese Funktion steht aktuell für Fileserver zur Verfügung. Über einen Klick auf die Kachel "Dateneigentümerbereich" und anschließend auf die Kachel "Fileserver", gelangt der Benutzer zum Dateneigentümermodus der Fileserver-Verwaltung. Für eine detaillierte Beschreibung dieser Funktion siehe auch [Verwaltung der Fileserver-Berechtigungen](#)(see page 269).

3.3.6 Genehmigungsworkflows



Über die Self-Service-Oberfläche ist auch der Zugriff auf die unterschiedlichen Kontexte der Genehmigungsworkflows möglich. Jeder Kontext wird direkt auf der Startseite angezeigt. In der Überschrift findet sich der Name des Kontext wieder - die große Ziffer unterhalb zeigt an, wieviele Requests in dem jeweiligen Kontext zur Genehmigung anstehen. Mit einem Klick auf die entsprechende Kachel gelangen Sie direkt zur Maske "Requests genehmigen" in dem jeweiligen Kontext.

4 Personenverwaltung

4.1 Personen

4.1.1 Allgemeines

Eine *Person* in tenfold ist nicht gleichzusetzen mit einem *Benutzer*. Die *Person* stellt in tenfold den physischen Menschen dar. Dieser kann über entsprechende Zuordnungen Ressourcen (wie beispielsweise Benutzerkonten in diversen Systemen) zugeordnet haben. Dies ermöglicht es tenfold mit der *Person* ein zentrales Objekt für Reports zur Verfügung zu stellen.

4.1.2 Personenarten

Jede Person ist einer bestimmten sogenannten *Personenart* zugeordnet. Die *Personenart* steuert wesentliche Elemente hinsichtlich des Ablaufs der Verwaltung. Für Details zur Konfiguration, siehe [Personen](#) (see page 63). Der Ablauf für die Verwaltung von Personen hängt hochgradig von der Systemkonfiguration ab. Beispielsweise kann in der Konfiguration vorgesehen werden, dass Personen bestimmter Personenarten automatisch aus einem Vorsystem, wie zum Beispiel einer Personalverwaltungssoftware, übernommen

werden. An diesem Punkt wird lediglich auf die manuelle Verwaltung von Personen über die tenfold-Oberfläche eingegangen.

4.1.3 Personen anlegen

Um eine Person anzulegen, wählen Sie im Menü den Punkt *Personen > Person anlegen* und anschließend den Unterpunkt, der jener Personenart entspricht, die angelegt werden soll. Bestimmte Personenarten können von der manuellen Verwaltung ausgeschlossen werden. In diesem Fall sind diese dann nicht über das Menü auswählbar. Diese Konfiguration wird häufig gewählt, wenn die betreffende Personenart durch eine Schnittstelle zu einem Vorsystem verwaltet wird.

Anschließend gelangen Sie auf die Folgemaske, dessen Aufbau konfigurationsabhängig ist. Nachfolgend sind alle möglichen Variationen dieser Maske beschrieben.

Überprüfung von existierenden Personen

The screenshot shows the tenfold web application interface. At the top, there's a navigation bar with the 'tenfold' logo and various menu items like 'Personen', 'Ressourcen', 'Berechtigungen', 'Requests', 'Organisation', 'Workflows', 'Provisioning', and 'Einstellungen'. Below the navigation bar, there's a header section for 'Neue Person der Art Externe Benutzer anlegen' with a 'Weiter' button and an 'Abbrechen' button. The main content area has three tabs: 'Prüfen', 'Benutzername', and 'Person anlegen'. The 'Prüfen' tab is selected, displaying a form titled 'Überprüfung von existierenden Personen'. This form contains two input fields: 'Vorname' and 'Nachname', both marked with a red asterisk. Below these fields is a blue button labeled 'Prüfen' with a circular arrow icon.

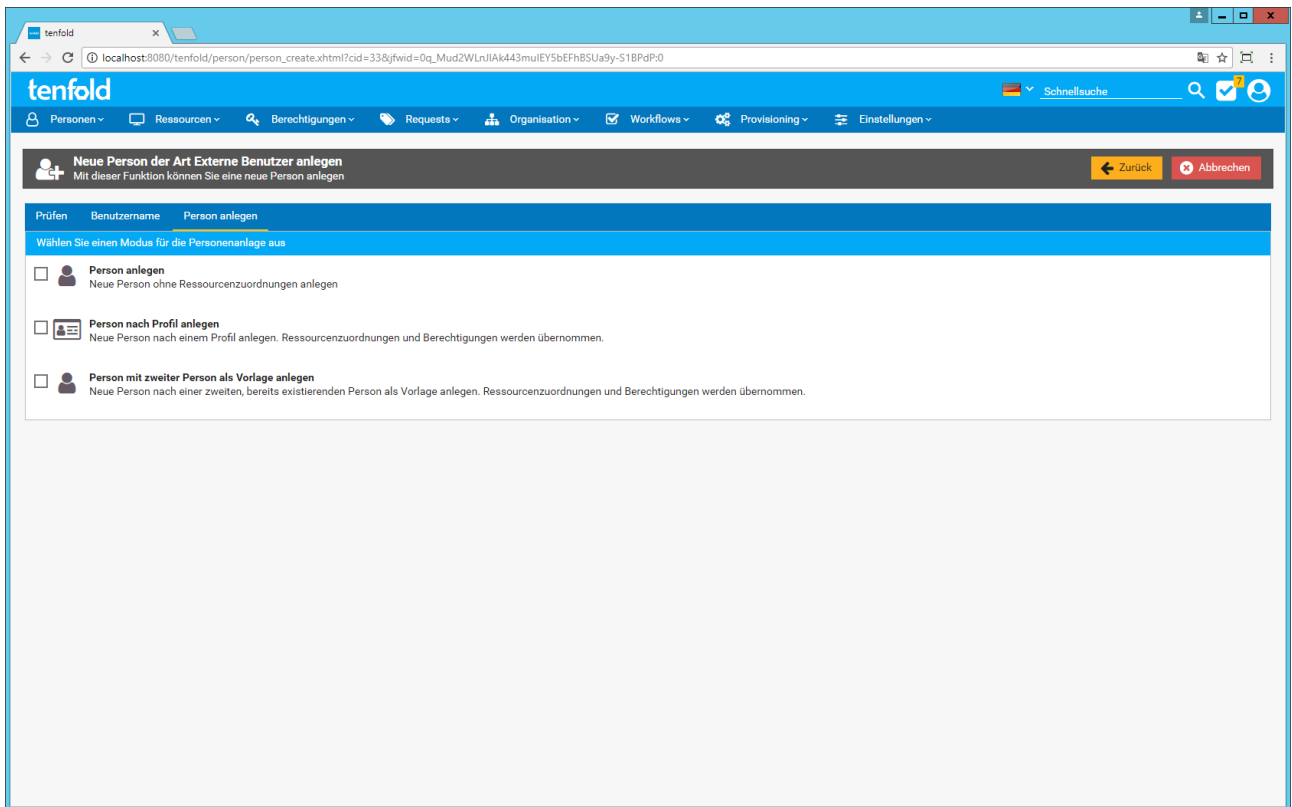
Die Überprüfung von existierenden Personen dient dazu, anhand einer Vor- und Nachnamenkombination zu überprüfen, ob eine bestimmte Person bereits in tenfold registriert ist. Um die Überprüfung durchzuführen, geben Sie Vor- und Nachnamen der anzulegenden Person ein und klicken Sie auf die Schaltfläche "Prüfen". Werden Personen gefunden, die auf den Namen zutreffen, so werden diese unter "Ähnliche Personen gefunden" aufgelistet. Ob es sich bei den gefundenen Personen um mögliche Namensduplikate handelt, kann, anhand der anderen angezeigten Daten (Benutzername, Personalnummer, Abteilung), überprüft werden. Sie können in der Tabelle über den Link "Bearbeiten" direkt auf die Maske "Person bearbeiten" springen, um Anpassungen an der jeweiligen Person vorzunehmen. Wird keine passende Person gefunden, entfällt die Tabelle.

Benutzername

The screenshot shows the tenfold web application interface. The main heading is "Neue Person der Art Externe Benutzer anlegen" (Create new external user of type). Below this, there are three tabs: "Prüfen", "Benutzername", and "Person anlegen". The "Benutzername" tab is active. The form contains a section "Benutzername vorschlagen" (Suggested username) with a text input field containing "franz.danz" and a "Prüfen" (Check) button. Below this, there is a section "Benutzername auswählen" (Select username) with a list of suggestions: "fdanz" and "franz.danz". The "franz.danz" suggestion is selected with a checkbox.

Der Abschnitt *Benutzername* dient der Festlegung des primären Benutzernamens der Person. Der primäre Benutzername in tenfold entspricht üblicherweise dem Benutzernamen der Person im Active Directory. Gegebenenfalls werden von tenfold bereits Benutzernamen vorgeschlagen, welche mit den relevanten Anwendungen auf Duplikate geprüft wurden. Aufgrund welcher Regeln der/die Benutzernamen vorgeschlagen werden und welche Systeme auf mögliche Duplikate geprüft werden ist konfigurationsabhängig.

Sie können einen der Vorschläge übernehmen, indem Sie den jeweiligen Eintrag in der Tabelle selektieren. Alternativ können Sie über das Textfeld und die Schaltfläche "Prüfen" einen eigenen Wunschnamen prüfen lassen und gegebenenfalls zur Auswahl hinzufügen. Ist der gewünschte Benutzername bereits in Verwendung, so erhalten Sie eine entsprechende Warnmeldung und der Name wird nicht zur Auswahl hinzugefügt.



Neue Person anlegen

Die Option "Neue Person anlegen" legt eine neue Person an, die keine vordefinierten Ressourcen- oder Berechtigungszuordnungen aufweist. Die Zuordnung eventueller Berechtigungen erfolgt anschließend vollständig auf manueller Basis.

Person nach Profil anlegen

Mit dieser Option ist es möglich, der neu anzulegenden Person initial bereits ein manuell ausgewähltes Profil zuzuordnen. Diese Option darf nicht mit der Möglichkeit verwechselt werden, dass der Person durch den Anlageprozess ein oder mehrere Profile regelbasiert zugeordnet werden. Die Zuordnung des bei dieser Option gewählten Profils erfolgt manuell und zusätzlich zu allen etwaigen, im Nachgang automatisch zugeordneten, Profilen.

Person mit zweiter Person als Vorlage anlegen

Diese Variante bietet die Möglichkeit, der neu anzulegenden Person die exakt gleichen Ressourcen und Berechtigungen wie einer bereits existierenden Person zuzuordnen.

Sicherheit

Es werden hierbei - ohne Filterung - *alle* Berechtigungen kopiert. Diese Option wird daher aus Sicherheitsgründen grundsätzlich nicht empfohlen.

Allgemeine Funktionen

Die nachfolgenden Funktionen stehen sowohl für die Anlage von neuen Personen als auch für die Bearbeitung von bereits existierenden Personen zur Verfügung. Bei Unterschieden wird entsprechend auf die Unterscheidung hingewiesen.

Stammdateneingabe

The screenshot shows the 'Person bearbeiten' interface in the tenfold application. The top navigation bar includes links for Personen, Ressourcen, Berechtigungen, Requests, Organisation, Workflows, Provisioning, and Einstellungen. The main header indicates the user is logged in as 'hans'. The form title is 'Person bearbeiten' with a subtitle 'Bearbeiten von Stammdaten und Anfordern von Ressourcen'. Action buttons for 'Ressourcen anfordern', 'Speichern', and 'Abbrechen' are visible. The 'Personendaten' tab is selected, showing the 'Stammdaten' section with the following fields:

Titel vor Name	-	Telefon *	+49 123123123
Vorname	Hans	Telefon 2	
Zweiter Vorname		Telefon Privat	
Nachname *	Sonne	Handy	
Titel nach Name	-	Fax	
Abteilung *	Verkauf	Personalnummer *	5874
Position *	Mitarbeiter	Kostenstelle	
Benutzername	hsonne	Personentyp *	Mitarbeiter
E-Mail	Hans.Sonne@tenfold.local		
Ablaufdatum			
Vorgesetzter	-		
Niederlassung *	München		

Aufbau

Der Aufbau der Maske ist in mehrfacher Hinsicht konfigurations- und berechtigungsabhängig:

- Der Aufbau des Karteireiters "Personendaten"
- Die Verfügbarkeit des Karteireiters "Ressourcen"

Im Karteireiter "Personendaten" müssen zunächst die Stammdaten für die anzulegende Person eingegeben werden. Je nach Konfiguration und Berechtigungen sind unterschiedliche Attribute für die Eingabe freigeschaltet bzw. zur verpflichtenden Eingabe vorgesehen.

Mussfelder

Attribute können in der Konfiguration als zwingende Attribute festgelegt werden. Diese sind mit einem kleinen roten Stern gekennzeichnet. Werden nicht alle zwingenden Attribute ausgefüllt bzw. eingegeben, so kann der Vorgang nicht abgeschlossen werden. Es erscheint eine entsprechende Warnmeldung neben dem/den betroffenen Attributen.

Datentypen

Bei der Eingabe können Sie auf unterschiedliche Datentypen treffen, deren Handhabung folgendermaßen ist:

Name	Verhalten	Beschreibung
Textfeld	Eingabe über Tastatur	Es handelt sich um ein Textfeld, in dem - je nach Konfiguration - freier Text eingegeben werden kann. Es kann sich beispielsweise um das Feld "Nachname" handeln.
Kalender	Auswahl eines Datums	Über den Kalender kann ein entsprechendes Datum (Tag) aus Insert gewählt werden. Eine manuelle Eingabe eines Datums in jeglicher Form ist nicht möglich.
Checkbox	Ja / Nein	Eine Checkbox kann angekreuzt werden (bedeutet "Ja") oder leer gelassen werden (bedeutet "nein").
Combobox	Auswahl einer Option	Es kann aus einer Liste von Optionen genau eine ausgewählt werden.
Multi-Select	Auswahl von mehreren Optionen	Es können aus einer Liste von Optionen entweder keine, eine oder mehrere Optionen gewählt werden. Aktuell steht dieser Datentyp nur für das Attribut "Niederlassung" zur Verfügung

Hinweise

Wenn dies in der Konfiguration vorgesehen wurde, kann für Attribute ein Hinweis hinterlegt werden. Dieser ist durch ein blaues Rufzeichen neben dem Attribut gekennzeichnet. Der Hinweis wird angezeigt, wenn Sie mit der Maus über dem blauen Rufzeichen verweilen.

Änderungen planen

Sofern es in der Personenart entsprechend konfiguriert wurde (siehe [Personenarten](#)(see page 81)), können Sie Änderungen nicht nur sofort durchführen, sondern auch für einen späteren Zeitpunkt planen. Damit wird dann sofort ein Request erzeugt, welcher jedoch für den angegebenen Zeitpunkt geplant und erst dann durchgeführt wird. Sollte die Möglichkeit für zukünftige Änderungen in der entsprechenden Personenart aktiviert sein, wird Ihnen über den Eingabefeldern zu den Stammdaten eine Schaltfläche "Neue zukünftige Änderung" eingeblendet.

Durch Betätigen dieser Schaltfläche öffnet sich ein Dialog, in welchem Sie das Durchführungsdatum für die Personenänderung eingeben können. Geben Sie hier das gewünschte Datum und die gewünschte Uhrzeit ein und betätigen Sie die Schaltfläche "Übernehmen". Sie können daraufhin die Stammdaten wie gewohnt eingeben, jedoch wird beim Speichern der Person der erstellte Request nicht sofort durchgeführt. Sollten Sie es sich anders überlegt haben, können Sie die zukünftige Änderung durch Betätigen der Schaltfläche "Neue zukünftige Änderung für <Datum> abbrechen" wieder stornieren. Ihre Änderungen werden dann sofort durchgeführt.

Zukünftige Daten

Während der Eingabemodus für zukünftige Änderungen aktiv ist, werden Ihnen nicht die aktuellen Daten der Person eingeblendet, sondern die Daten, welche zum Durchführungsdatum der Person aktiv sein werden, sollten weitere zukünftige Änderungen bereits geplant sein. Ob Sie hier die Daten für alle bis dahin geplanten Requests sehen oder nur von jenen, die bereits genehmigt wurden, können Sie in den Systemparametern (siehe [Systemparameter](#)(see page 484)) konfigurieren.

Nachdem Sie die Änderungen gespeichert und geplant haben, können Sie die Schaltfläche "Neue zukünftige Änderung" erneut betätigen, um eine weitere zukünftige Änderung zu planen. Sie können damit gleich eine ganze Reihe an Änderungen für die Zukunft planen.

Wenn Sie bereits zukünftige Änderungen geplant haben, steht Ihnen eine weitere Schaltfläche, "<X> geplante Änderungen", zur Verfügung. Mit einem Klick auf diese Schaltfläche öffnen Sie einen Dialog, in welchem Sie sich alle geplanten Änderungen anzeigen lassen können und diese auch abbrechen können (sofern Sie über die entsprechende Berechtigung zum Abbrechen von Requests verfügen, siehe [Berechtigungen](#)(see page 457)).

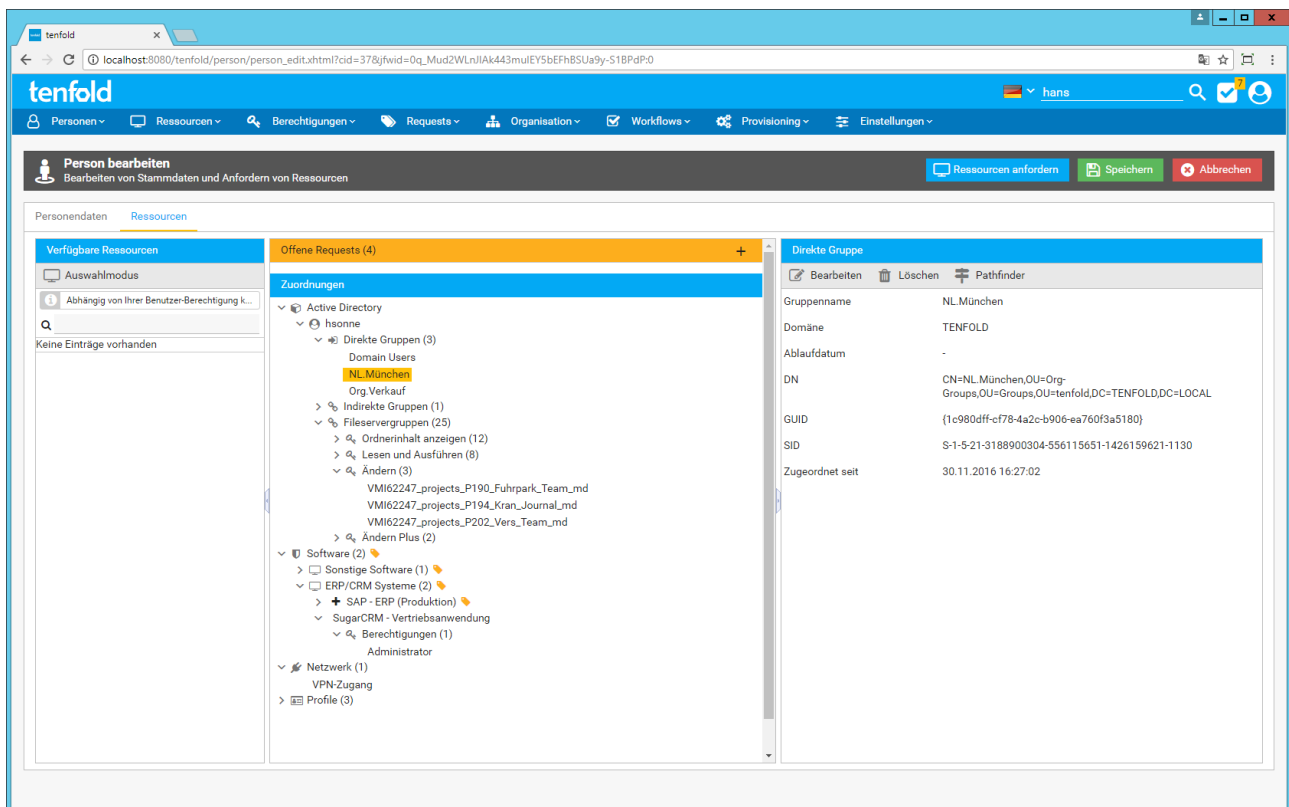
Legacy-Modus für zukünftige Änderungen

Neben dieser Möglichkeit zur Planung von zukünftigen Änderungen gibt es auch noch den Legacy-Modus (siehe [Personenarten](#)(see page 81)) für zukünftige Änderungen. In diesem Modus werden Sie, beim Betätigen der Schaltfläche "Speichern", gefragt, ob die Änderung sofort oder an einem späteren Zeitpunkt durchgeführt werden soll. Dieser Modus ist dafür gedacht, Benutzern, welche bereits die alte Variante verwendet haben, weiterhin die gewohnte Art der zukünftigen Änderungen zu bieten. Der größte Nachteil dieser Variante ist, dass Sie beim Bearbeiten der Daten die aktuellen Personendaten sehen und nicht die Personendaten, welche zum Zeitpunkt der Änderung aktiv sind. Es wird daher empfohlen, die neue Art für die Planung zukünftiger Änderungen zu verwenden.

Ressourcen

Benötigte Berechtigung

Um die Ressourcenzuordnungen anzuzeigen, benötigen Sie die Berechtigung "Ressourcen anzeigen" für die entsprechende Personenart. Zur Bearbeitung der Zuordnungen benötigen Sie die Berechtigung "Ressourcen anfordern" der entsprechenden Personenart.



Begriff "Ressource"

Der Begriff "Ressource" wird hier - wie an den meisten Stellen der Dokumentation - sowohl als Begriff für eigentliche Ressourcen (Menü "Ressourcen") als auch für andere Elemente genutzt, die einer Person zugeordnet werden können. Unter "Ressourcen" werden somit auch Anwendungsberechtigungen, Active Directory/Microsoft 365-Gruppen oder Profile verstanden.

Aufbau

Der Karteireiter "Ressourcen" wird ebenfalls, abhängig von Konfiguration und Berechtigung, angezeigt. Auf diesem Karteireiter ist es möglich, der Person Ressourcen aller Art zuzuordnen oder zu entziehen. Die Maske ist grundsätzlich in mehrere Bereiche gegliedert:

- Der linke Bereich, "Suche" bzw. "Auswahl", ermöglicht die Suche bzw. die Auswahl von Ressourcen, die dem Benutzer neu zugeordnet werden sollen.
- Der obere Bereich, "Offene Requests" bzw. "Neue Requests", zeigt alle bereits gespeicherten Requests zur Person ("Offene Requests") und alle im aktuellen Vorgang zu erstellende Requests ("Neue Requests") an.
- Der mittlere Bereich, "Zuordnungen", dient der Darstellung der aktuell zugeordneten Ressourcen.
- Der rechte Bereich (Detailbereich) zeigt Details zum aktuell selektierten Objekt an und lässt Änderungen zu diesem Objekt zu (beispielsweise kann hier eine Zuordnung gelöscht oder bearbeitet werden).

Neue Ressource zuordnen

Um der Person ein neues Objekt zuzuordnen, muss dieses per Drag & Drop vom linken Such- oder Auswahlbereich in den rechten Bereich "Zuordnungen" gezogen werden. Der Suchmodus für Objekte verhält sich grundsätzlich unterschiedlich zum Auswahlmodus für Objekte:

- Suchmodus: Man erkennt, dass man sich im Suchmodus befindet, wenn im linken Bereich ein Textfeld mit einer Lupe sichtbar ist. Im Textfeld muss der exakte Name oder ein Teil des Namens des Objekts eingegeben werden. Durch die Eingabe wird automatisch das Suchergebnis aktualisiert. Nach dem Ziehen (Drag & Drop) des Objektes in den mittleren Bereich "Zuordnungen" scheint dieses dort mit einem Plusymbol auf, was bedeutet, dass dieses Objekt nach dem Speichern neu zugeordnet wird.
- Auswahlmodus: In den Auswahlmodus gelangen Sie, indem Sie im Suchmodus auf den Button "Auswahlmodus" klicken. Im Auswahlmodus werden die Objekte in unterschiedlichen Abschnitten aufgelistet. Der Abschnitt "Empfohlene Ressourcen" enthält alle Ressourcen, die entsprechend gekennzeichnet wurden (der Abschnitt wird nur angezeigt, wenn zumindest eine Ressource als "empfohlene Ressource" gekennzeichnet wurde). Darunter werden alle Ressourcen in Abschnitten, die analog zur Ressourcenkategorie sind, angezeigt. Darunter wiederum befindet sich ein Abschnitt, welcher alle Profile beinhaltet. Andere Objekte wie Active Directory-Gruppen werden, aufgrund der hohen Datenmenge, im Auswahlmodus nicht angezeigt.

Tipp

Die Einstellung, ob Sie sich im Auswahl- oder Suchmodus befinden, wird in den Benutzereinstellungen gespeichert. Wenn Sie die Maske das nächste Mal aufrufen, gelangen Sie automatisch in den Modus, den Sie zuletzt verwendet haben.

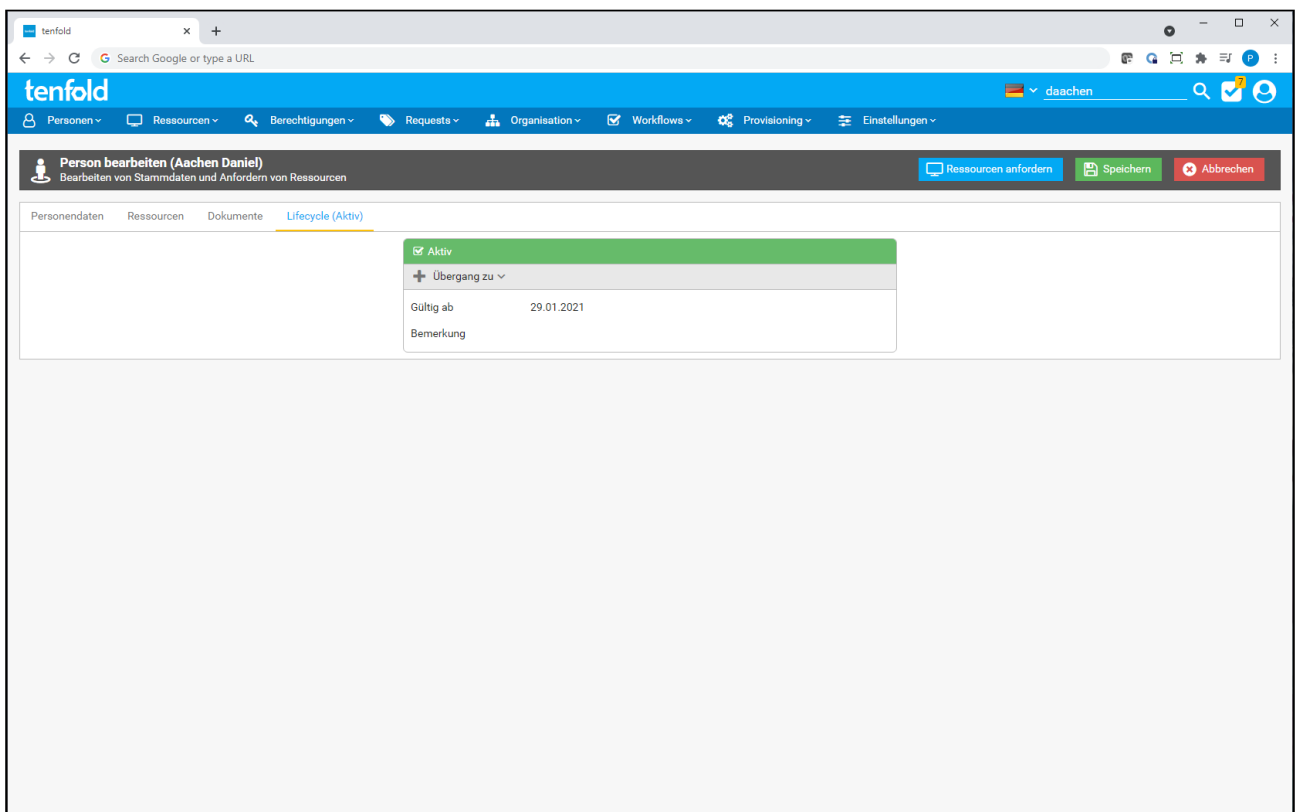
Bestehende Ressource löschen

Eine bereits bestehende Zuordnung kann grundsätzlich gelöscht werden, indem im rechten Bereich ("Zuordnungen") die betroffene Ressource in der Baumansicht per Mausklick selektiert wird und anschließend im rechten Bereich (Detailbereich) in der Toolbar der Punkt "Löschen" angewählt wird. Die bevorstehende Löschung wird durch ein rotes Kreuzsymbol gekennzeichnet. Im oberen Bereich ("Neue Requests") wird ein dementsprechender Eintrag angezeigt.

Lifecycle

Benötigte Berechtigung

Für die Anzeige der aktuellen Lifecycle-Phase benötigen Sie die Berechtigung "Lifecycle anzeigen" der entsprechenden Personenart. Zur Bearbeitung benötigen Sie die Berechtigung "Lifecycle anfordern" der Personenart.



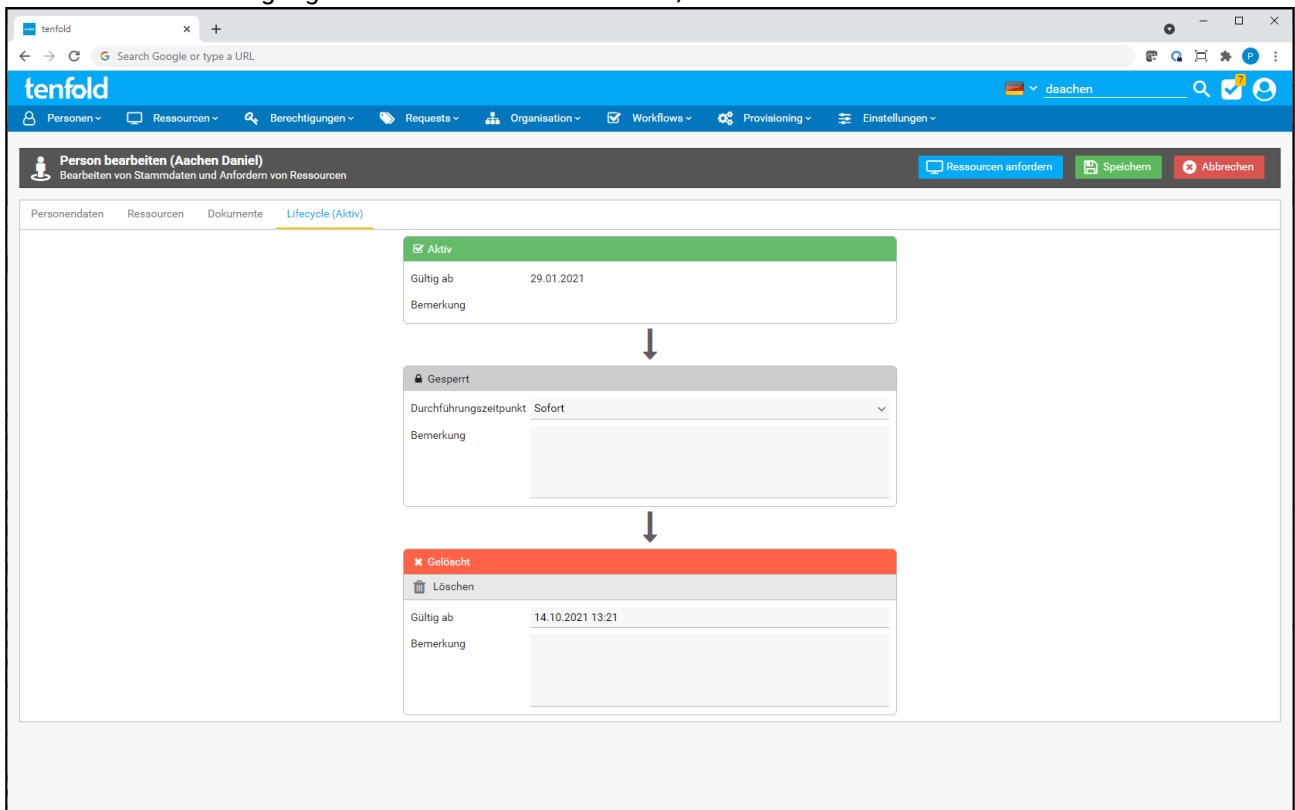
Im Kartereiter "Lifecycle" finden Sie die aktuelle Lifecycle-Phase der Person. Sie erhalten außerdem folgende Informationen:

Information	Beschreibung
Gültig ab	Gibt an, seit wann sich diese Person in der aktuellen Lifecycle-Phase befindet.
Bemerkung	Hier sehen Sie den Kommentar, welcher zur Anforderung der aktuellen Phase eingegeben wurde, sofern vorhanden.
Automatischer Phasenwechsel	Zeigt an, zu welchem Zeitpunkt ein automatischer Phasenwechsel in welche Phase stattfindet. Diese Information wird nur dann angezeigt, wenn ein automatischer Phasenwechsel bevorsteht.

Aktuelle Phase

Der Name der aktuellen Phase wird auch im Titel des Kartereiters "Lifecycle" in Klammern angezeigt.

Um einen manuellen Wechsel von der aktuellen Phase in eine andere Phase durchzuführen, verwenden Sie die Schaltfläche "Übergang zu" und wählen die Phase aus, in welche die Person überführt werden soll.



Phasenwechsel

Welche Phasenwechsel zulässig sind kann für jede Phase individuell definiert werden. Sollte kein Phasenwechsel angeboten werden, könnte dies daran liegen, dass für diese Phase kein möglicher Wechsel definiert wurde. Dies ist zum Beispiel für die Phase "Gelöscht" der Fall.

Es wird daraufhin ein weiterer Bereich für die Folgephase angezeigt. In diesem können Sie folgende Einstellungen vornehmen:

Einstellung	Beschreibung
Durchführungszeitpunkt	Wählen Sie hier aus, ob der Phasenwechsel sofort oder in der Zukunft stattfinden soll.
Gültig ab	Gibt den genauen Zeitpunkt an, zu welchem der Phasenwechsel durchgeführt werden soll. Diese Einstellung ist nur sichtbar, wenn in der Einstellung "Durchführungszeitpunkt" die Auswahl "Spezifischer Zeitpunkt" gewählt wurde.
Bemerkung	Ein Kommentar, welcher angegeben werden kann, um die Hintergründe des Phasenwechsels zu erläutern. Dieser Kommentar wird sowohl im Request des Phasenwechsels angezeigt als auch auf dieser Maske, sobald der Phasenwechsel durchgeführt wurde.

Sie können an dieser Stelle beliebig viele Phasenwechsel planen. Verwenden Sie hierfür die Schaltfläche "Übergang zu", welche sich im Bereich der neuen Phase befindet. Jeder weitere hinzugefügte Phasenwechsel muss zeitlich später, als der vorhergehende angesetzt werden.

Rückkehr aus Abwesenheit

Sollten Sie die Abwesenheitsdauer einer Person kennen, können Sie dies zum Beispiel benutzen, um gleich mit der Sperre die Reaktivierung zu planen. So stellen Sie sicher, dass nicht vergessen wird, die Person rechtzeitig zu reaktivieren.

Dokumente

Benötigte Berechtigung

Zur Anzeige (und zum Herunterladen) der Dokumente benötigen Sie die Berechtigung "Dokumente Anzeigen" der jeweiligen Personenart. Um neue Dokumente über diese Maske hochladen zu können benötigen Sie die Berechtigung "Dokumente Hochladen". Zum Löschen bestehender Dokumente wird die Berechtigung "Dokumente Löschen" benötigt.

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 header indicates 'Person bearbeiten (Aachen Daniel)' with subtext 'Bearbeiten von Stammdaten und Anfordern von Ressourcen'. Below this, there are tabs for 'Personendaten', 'Ressourcen', 'Dokumente' (selected), and 'Lifecycle (Aktiv)'. A '+ Dokument hochladen' button is visible. The 'Dokumente' tab displays a table with the following data:

Name	Erstellt von	Erstellungsdatum	Größe
leumundzeugnis.pdf	Admin tenfold (systemfold)	14.10.2021 14:24:40	25,09 KB
sicherheitsrichtlinie-unterzeichnet.pdf	Admin tenfold (systemfold)	14.10.2021 14:21:08	25,09 KB

Auf dem Karteireiter "Dokumente" befinden sich sämtliche Dokumente, welche der Person angehängt wurden. Dies kann durch interaktive Aktivitäten oder durch das Verwenden dieser Maske geschehen. Hierbei kann es sich, zum Beispiel, um unterschriebene Geheimhaltungsvereinbarungen oder ähnliche Dokumente halten, die für die Sicherheitsrichtlinien relevant sind.

Um ein neues Dokument an die Person zu hängen, betätigen Sie die Schaltfläche "Dokument hochladen".

Daraufhin erscheint ein Dialog, in dem Sie eine oder mehrere Dateien hochladen können. Bestätigen Sie Ihre

Auswahl durch die Schaltfläche "Übernehmen". Neu hinzugefügte Dateien werden mit einem Plus-Symbol markiert. Die Dateien werden erst beim Speichern der Person endgültig angehängt. Um ein Dokument zu entfernen, wählen Sie die Aktion "Löschen" im Aktionsmenü des jeweiligen Dokumentes. Zu löschende Dokumente werden mit einem X-Symbol markiert. Beim Speichern der Person werden diese entfernt.

Gelöschte Dokumente

Gelöschte Dokumente werden auf dieser und anderen Maske lediglich ausgeblendet. Die eigentlichen Daten bleiben in der Datenbank, zu Zwecken der Historie, erhalten.

Dokumentenablage

Es können an dieser Stelle beliebige Dokumente angehängt werden. Beachten Sie jedoch, dass tenfold nicht als allgemeine Dokumentenablage gedacht ist. Beschränken Sie sich daher auf Dokumente, die sicherheits- oder prozessrelevant sind. Um ein Ausufern der angehängten Daten zu vermeiden, können Sie die mögliche Anzahl der angehängten Dokumente pro Person mittels des Systemparameters *Datei-Uploads > Personendokumente > Anzahl Personendokumente* auf der Maske *Einstellungen > Systemparameter* beschränken. Zusätzlich kann die Maximale Größe der Personendokumente mit dem Systemparameter *Datei-Uploads > Personendokumente > Personendokument-Größe* beschränkt werden.

Speichern

Wenn alle Einstellungen vorgenommen wurden, so können Sie den Vorgang über die Schaltfläche "Speichern" abschließen. Der übliche weitere Ablauf gestaltet sich wie folgt:

- Wurden Personendaten angelegt oder bearbeitet, wird ein Request zur Anlage der neuen oder geänderten Person angelegt. Je nach Workflow-Konfiguration muss dieser Request erst durch die zuständigen Stellen genehmigt werden, bevor es zu einer tatsächlichen Änderung kommt.
- Es werden Requests für die Zuordnung der ausgewählten Ressourcen angelegt. Je nach Workflow-Konfiguration müssen diese Requests erst durch die zuständigen Stellen genehmigt werden, bevor es zu einer tatsächlichen Zuordnung kommt.
- Wurden Lifecycle-Phasenwechsel eingetragen, werden die notwendigen Requests angelegt, welche notwendig sind, um die Wechsel durchzuführen. Je nach Einstellungen in den Lifecycle-Phasen kann es notwendig sein, dass diese Requests erst genehmigt werden müssen.
- Neu hochgeladene Personendokumente werden gespeichert. **Hinweis:** Hierfür werden **keine** Requests angelegt.

Konfiguration

Grundsätzlich kann der Ablauf durch die Systemkonfiguration jedoch hochgradig individuell angepasst werden.

4.1.4 Personen bearbeiten

Um eine Person bearbeiten zu können gibt es mehrere Einsprungspunkte. Dies gilt auch für alle nachfolgenden Funktionen, wie beispielsweise das Sperren.

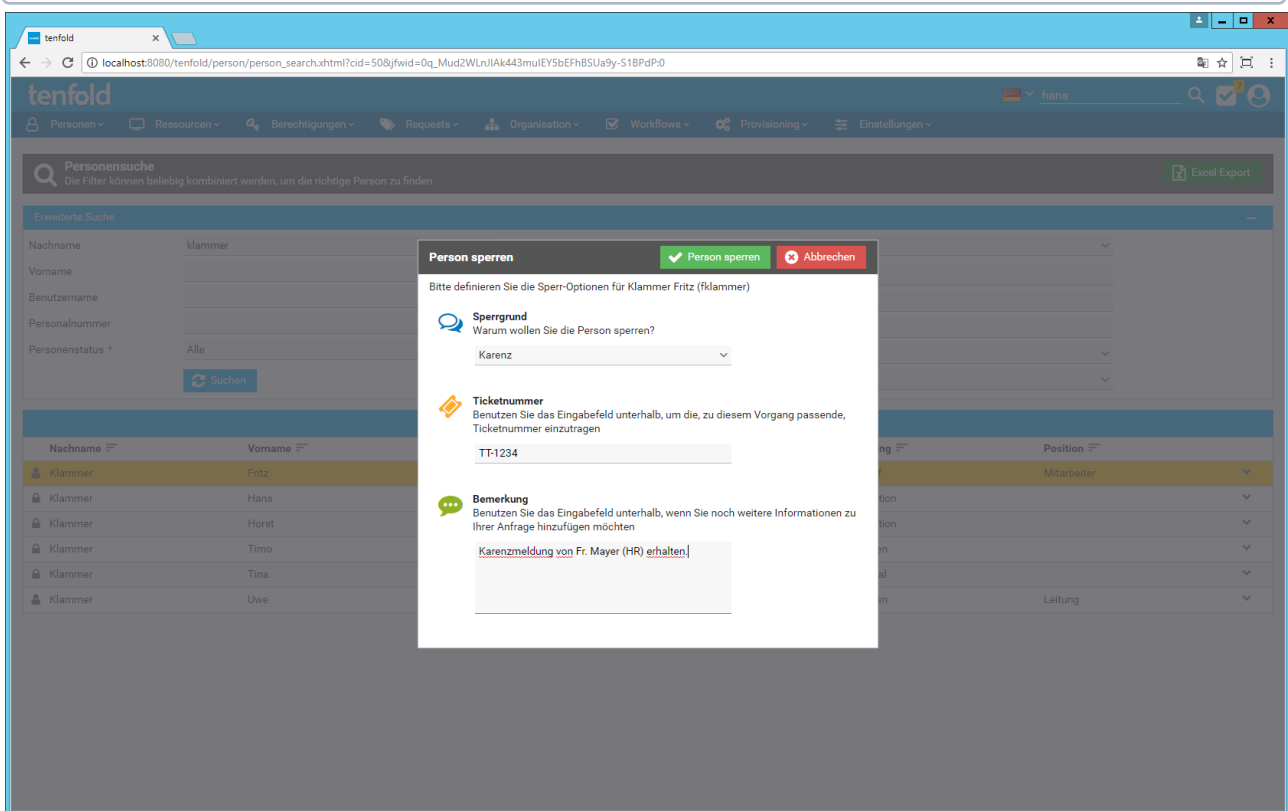
- Die Person wird über die Schnellsuche gesucht und bearbeitet (siehe [Personen](#)(see page 63)).
- Die Person wird über die Personensuche gesucht und bearbeitet (siehe [Personen](#)(see page 63)).

Der Ablauf für die Bearbeitung einer Person ist analog zur Neuanlage.

4.1.5 Personen sperren

Legacy

Die Aktion "Person sperren" ist ein Legacy-Feature von tenfold. In neuen Installationen von tenfold oder nach einer Migration auf Lifecycle-Phasen ist diese Aktion nicht mehr verfügbar. Ändern Sie die Lifecycle-Phase der Person in "Gesperrt", um dasselbe Ergebnis mit dem Lifecycle-Feature zu erzielen.



Eine Person kann in tenfold gesperrt werden. Eine Sperre ist dann durchzuführen, wenn einer Person nur temporär der Zugang zu ihren zugeordneten Ressourcen entzogen werden soll. Bei einer Sperre ist grundsätzlich davon auszugehen, dass die Person zu einem späteren Zeitpunkt wieder Zugriff erhalten soll. Auch dieser Vorgang wird gegebenenfalls nicht unmittelbar durchgeführt, sondern in einem Request abgebildet. Dieser Request unterliegt gegebenenfalls einem Genehmigungs-Workflow. Für die Sperren können grundsätzliche folgende Einstellungen genutzt werden:

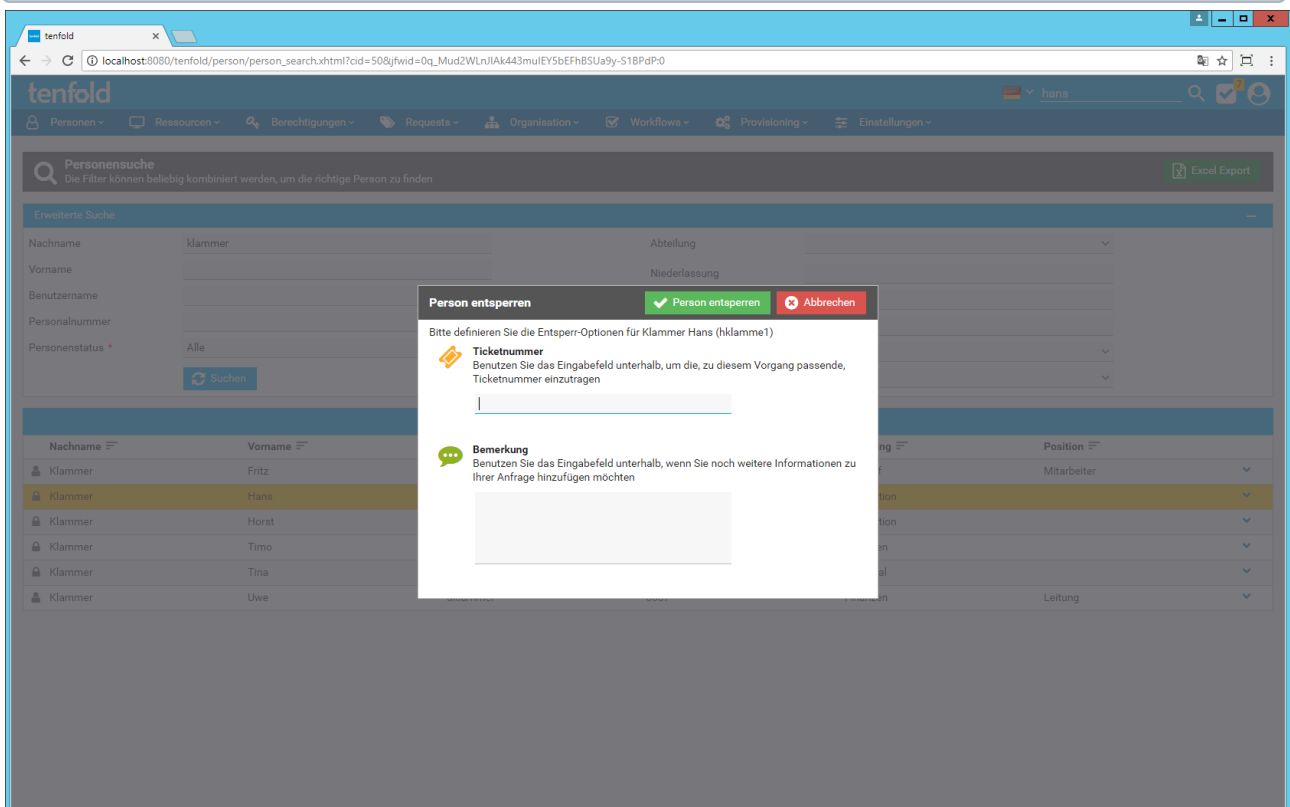
- Sperrgrund: Hier kann festgelegt werden, aus welchem Grund die Sperre erfolgt. Typische Gründe sind: Karenz, Krankenstand oder Ähnliches (konfigurationsabhängig; siehe auch [Request-Begründungen](#)(see page 63)).
- Ticketnummer: Es gibt die Möglichkeit, hier die Ticketnummer zu hinterlegen, mit der die Anfrage initial im Help-Desk-System gestellt wurde (konfigurationsabhängig; siehe auch [Personen](#)(see page 63)).

- Bemerkung: An dieser Stelle kann man eine zusätzliche Bemerkung hinterlegen. Diese Informationen erhalten die beteiligten Personen im Genehmigungs-Workflow.

4.1.6 Personen entsperren

Legacy

Die Aktion "Person entsperren" ist ein Legacy-Feature von tenfold. In neuen Installationen von tenfold oder nach einer Migration auf Lifecycle-Phasen ist diese Aktion nicht mehr verfügbar. Ändern Sie die Lifecycle-Phase der Person in "Aktiv", um dasselbe Ergebnis mit dem Lifecycle-Feature zu erzielen.



Das Entsperrn einer Person stellt den Zugriff auf die zugeordneten Ressourcen wieder her. Es können lediglich Personen entsperrt werden, welche zuvor gesperrt waren. Auch die Entsperrung wird gegebenenfalls nicht unmittelbar durchgeführt, sondern in einem Request abgebildet. Dieser Request unterliegt gegebenenfalls einem Genehmigungs-Workflow. Für das Entsperrn können grundsätzlich folgende Einstellungen vorgenommen werden:

- Entsperrungsgrund: Hier kann festgelegt werden, aus welchem Grund die Entsperrung erfolgt. Typische Optionen sind: Rückkehr aus Karenz oder Krankenstand oder Ähnliches (konfigurationsabhängig; siehe auch [Request-Begründungen](#)(see page 63)).
- Ticketnummer: Es gibt die Möglichkeit hier die Ticketnummer zu hinterlegen, mit der die Anfrage initial im Help-Desk-System gestellt wurde (konfigurationsabhängig; siehe auch [Personen](#)(see page 63)).
- Bemerkung: An dieser Stelle kann man eine zusätzliche Bemerkung hinterlegen. Diese Informationen erhalten die beteiligten Personen im Genehmigungs-Workflow.

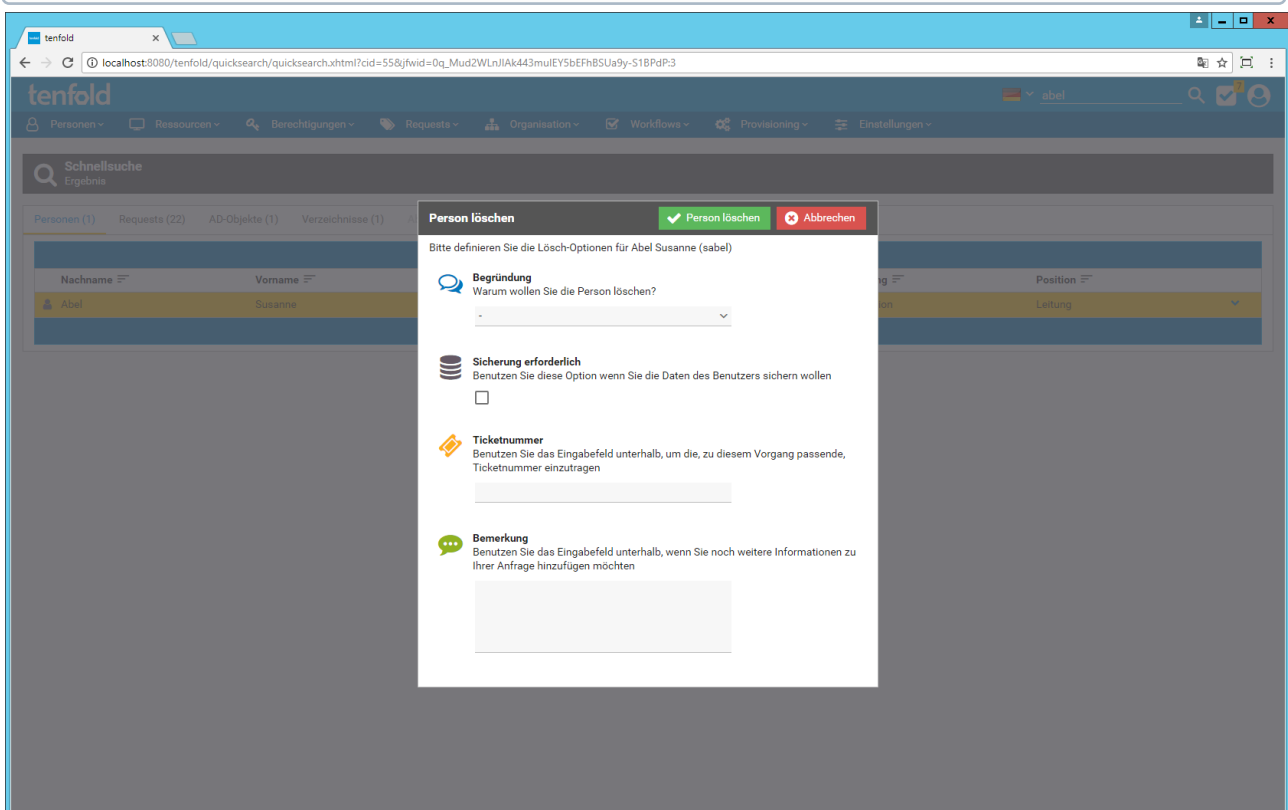
Request-Begründung

Die Hinterlegung eines Entsperrungsgrundes ist nicht vorgesehen.

4.1.7 Personen löschen

Legacy

Die Aktion "Person sperren" ist ein Legacy-Feature von tenfold. In neuen Installationen von tenfold oder nach einer Migration auf Lifecycle-Phasen ist diese Aktion nicht mehr verfügbar. Ändern Sie die Lifecycle-Phase der Person in "Gelöscht", um dasselbe Ergebnis mit dem Lifecycle-Feature zu erzielen.



Das Löschen einer Person hat tiefgreifendere Auswirkungen als das Sperren. Gelöschte Personen können nicht mehr reaktiviert und/oder bearbeitet werden. Lediglich sämtliche Auswertungsfunktionen (Berichte, Historie und Ähnliches) stehen für gelöschte Personen zur Verfügung. Gelöschte Personen werden in allen Listen und Anzeigefunktionen in tenfold ausgeblendet. Die einzige Möglichkeit, gelöschte Personen zu finden, besteht über die Schnellsuche, indem die Option "Gelöschte Personen" zusätzlich aktiviert wird. Die Löschung wird gegebenenfalls nicht unmittelbar durchgeführt, sondern in einem Request abgebildet. Dieser Request unterliegt gegebenenfalls einem Genehmigungs-Workflow. Für das Löschen können grundsätzlich folgende Einstellungen vorgenommen werden:

- **Begründung:** Hier kann festgelegt werden, aus welchem Grund die Löschung erfolgt. Typische Optionen sind: Kündigung, Entlassung oder Ähnliches (konfigurationsabhängig; siehe auch [Request-Begründungen](#)(see page 63)).

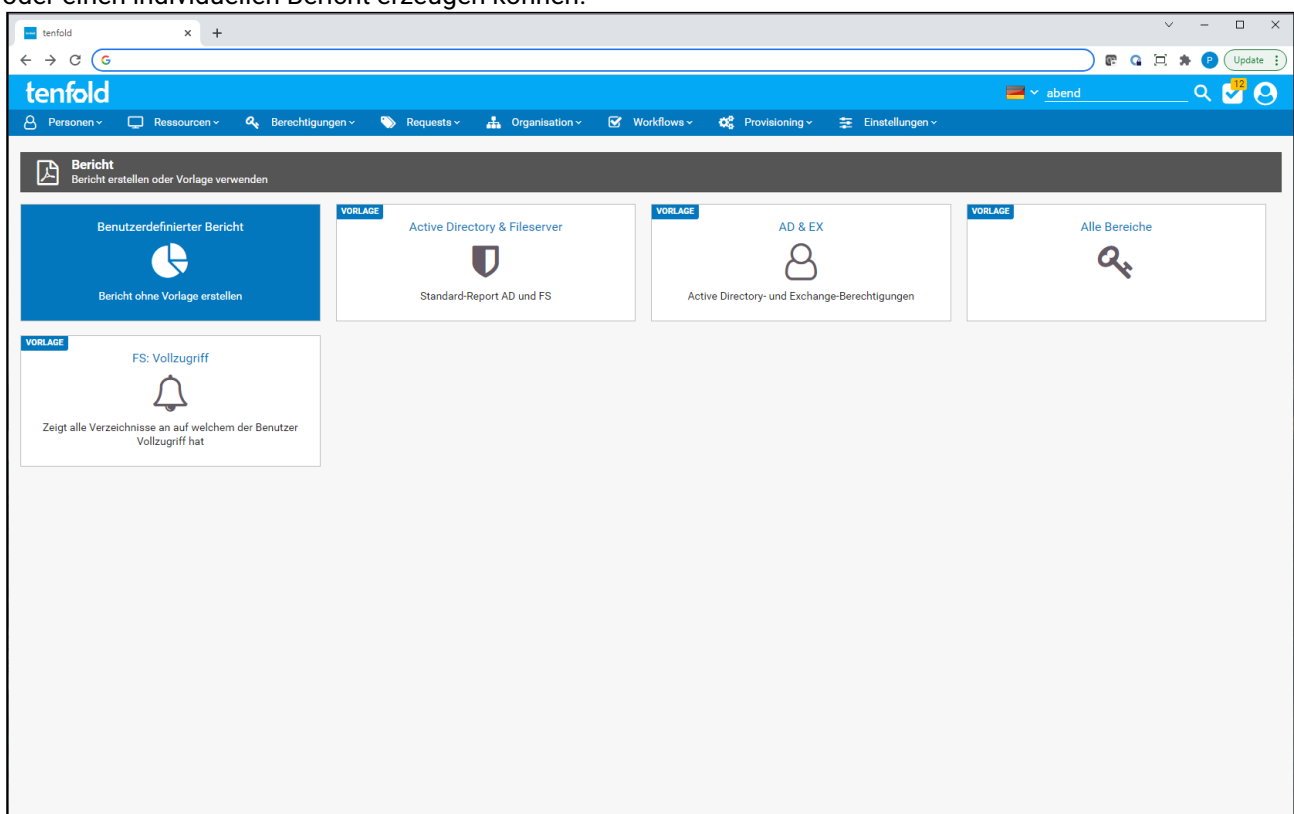
- Sicherung erforderlich: Durch dieses Kennzeichen kann vermerkt werden, dass die Daten des Benutzers gesichert werden sollen.
- Ticketnummer: Es gibt die Möglichkeit hier, die Ticketnummer zu hinterlegen, mit der die Anfrage initial im Help-Desk-System gestellt wurde (konfigurationsabhängig; siehe auch [Personen](#)(see page 63)).
- Bemerkung: An dieser Stelle kann man eine zusätzliche Bemerkung hinterlegen. Diese Informationen erhalten die beteiligten Personen im Genehmigungs-Workflow.

4.1.8 Berichte

Sie haben in tenfold die Möglichkeit, Berichte über die Berechtigungen von Personen anzulegen, um diese drucken oder versenden zu können. Oftmals wünschen externe Auditoren eine Übersicht über die Berechtigungen verschiedener Konten, haben jedoch keinen Zugang zu tenfold. In diesem Fall können Berichte erzeugt werden, um den Auditoren die gewünschten Informationen zukommen lassen zu können. Es steht Ihnen hierbei eine Vielzahl von Optionen zur Verfügung, um zu steuern, welche Daten in den erzeugten Berichten ersichtlich sind.

Neuen Bericht erzeugen

Um einen neuen Bericht zu erzeugen, wählen Sie die Aktion "Bericht" im Aktionsmenü einer Person auf einer der verschiedenen Suchmasken von tenfold (siehe [Schnellsuche](#)(see page 350), siehe [Personensuche](#)(see page 357)). Sie gelangen daraufhin zu einer Übersichtsmaske, wo Sie eine bestehende Berichtsvorlage auswählen oder einen individuellen Bericht erzeugen können.

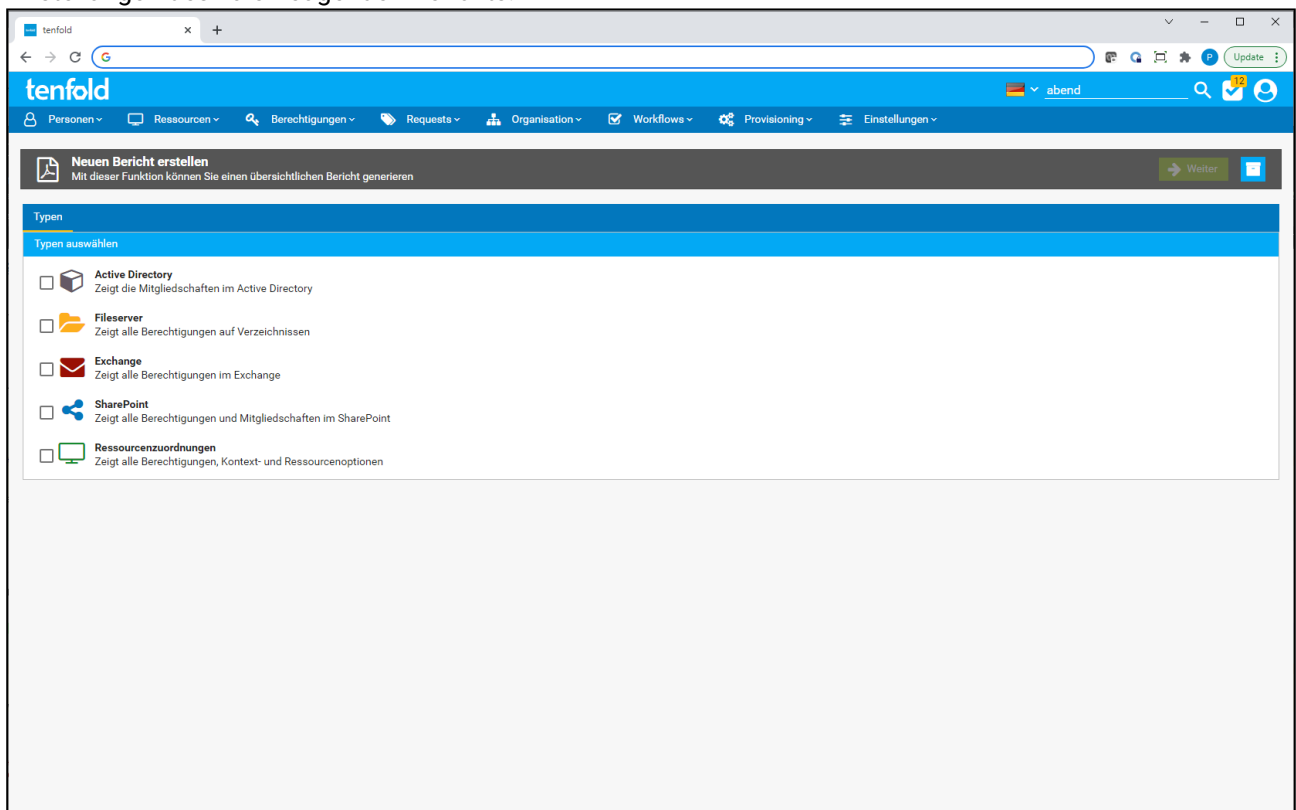


Keine Berichtsvorlagen

Sollten keine Berichtvorlagen verfügbar sein, gelangen Sie direkt zur Eingabemaske für benutzerdefinierte Berichte.

Klicken Sie an dieser Stelle auf die Kachel von einer der vorgeschlagenen Berichtsvorlagen, um einen Bericht mit den dort getroffenen Einstellungen zu erzeugen oder klicken Sie auf "Benutzerdefinierter Bericht", um einen neuen Bericht mit eigenen Einstellungen zu erzeugen.

Wenn Sie "Benutzerdefinierter Bericht" gewählt haben, gelangen Sie auf die Eingabemaske für die Einstellungen des zu erzeugenden Berichts.



Zunächst erhalten Sie die Möglichkeit, die Bereiche auszuwählen, welche in dem Bericht enthalten sein sollen.

Bereich	Beschreibung
Active Directory	Enthält Gruppenmitgliedschaften im Active Directory (ausgenommen Berechtigungsgruppen von Fileservern, Exchange und SharePoint)
Fileserver	Enthält Berechtigungen auf den Fileservern. Dies beinhaltet Berechtigungen mittels Fileservergruppen, anderen Gruppen oder direkt gesetzten Berechtigungen auf dem Dateisystem.
Exchange	Enthält Berechtigungen auf Postfächern und Ordnern in Exchange-Servern. Dies inkludiert Berechtigungen mittels Berechtigungsgruppen und direkt vergebenen Berechtigungen.
SharePoint	Enthält alle Berechtigungen auf SharePoint-Objekten. Dies inkludiert Berechtigungen mittels Berechtigungsgruppen und direkt vergebenen Berechtigungen.

Bereich	Beschreibung
Ressourcenzuordnungen	Enthält alle Ressourcenzuordnungen, deren Optionen und vergebenen Berechtigungen in tenfold.

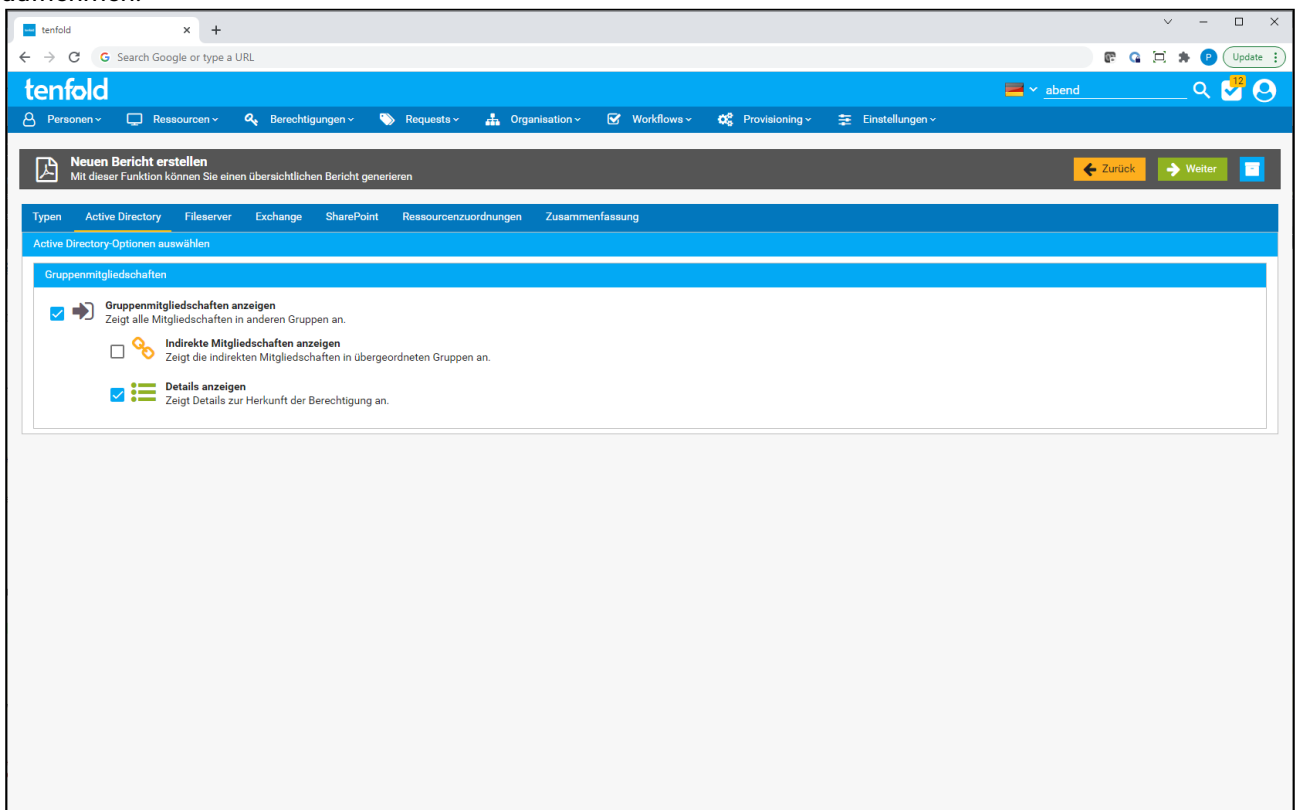
Wählen Sie einen oder mehrere Bereiche aus und Klicken Sie anschließend auf "Weiter" im Kopfbereich der Maske.

Weiter

Sie müssen zumindest einen der Bereiche ausgewählt haben, bevor Sie die Schaltfläche "Weiter" betätigen können.

Active Directory

Mittels des Bereichs "Active Directory" können Sie die Gruppenmitgliedschaften der Person in den Bericht mit aufnehmen.



4.2 Personenarten

4.2.1 Allgemeines

Personenarten steuern viele wesentliche Abläufe für Personen, die dieser Art zugeordnet sind. Jede Person ist zu einem bestimmten Zeitpunkt nur einer Art zugeordnet.

Zu den Einstellungen, die von Personenarten gesteuert werden, zählen, unter anderem:

- Grundeinstellungen wie Name, Icon, Beschreibung und Grundfunktionen

- Konfiguration der Genehmigungsworkflows für Anlagen, Änderungen und andere Operationen zu einer Person
- Zusammenstellung und Konfiguration der Felder (Attribute), die für Personen dieser Art gespeichert werden können

4.2.2 Anzeige

Die Verwaltung der Personenarten kann über das Menü unter *Personen* > *Stammdaten* > *Personenarten* erreicht werden.

Benötigte Berechtigung

Für die Verwaltung ist die Berechtigung "Manage Person Types" (1120) erforderlich.

Name	Beschreibung	Personen-Icon	Mehrere Niederlassungen	Benötigte Berechtigung	Standard
Extern		external-link	-	Z: Verwaltung Testbenutzer	-
Mitarbeiter	Standardperson	user	-	Z: Verwaltung Mitarbeiter	✓
Testbenutzer	Test	user-circle	-	Z: Verwaltung Testbenutzer	-

Es werden alle im System konfigurierten Arten angezeigt. Eine neue Art kann über den Button "Neu" angelegt werden. Bestehende Arten können über das Kontextmenü der jeweiligen Zeile bearbeitet oder gelöscht werden.

4.2.3 Anlegen oder Bearbeiten

Die Masken für das Anlegen oder das Bearbeiten einer Personenart sind identisch und bestehen aus mehreren Karteireitern, auf denen Einstellungen vorgenommen werden können:

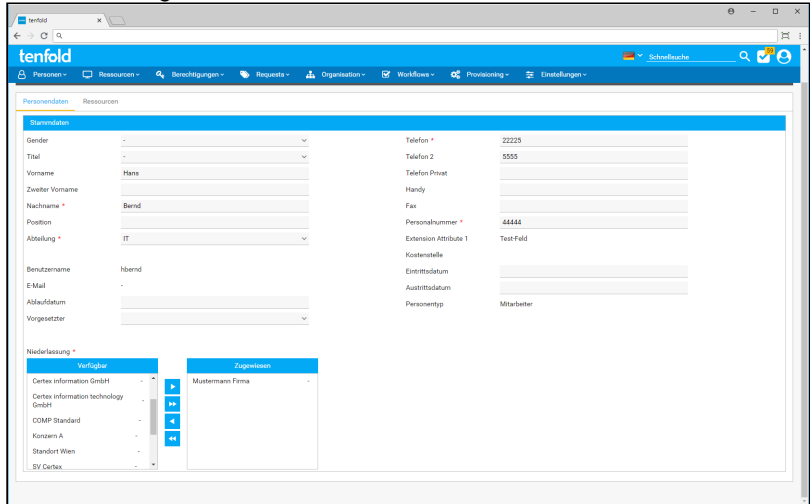
Allgemein

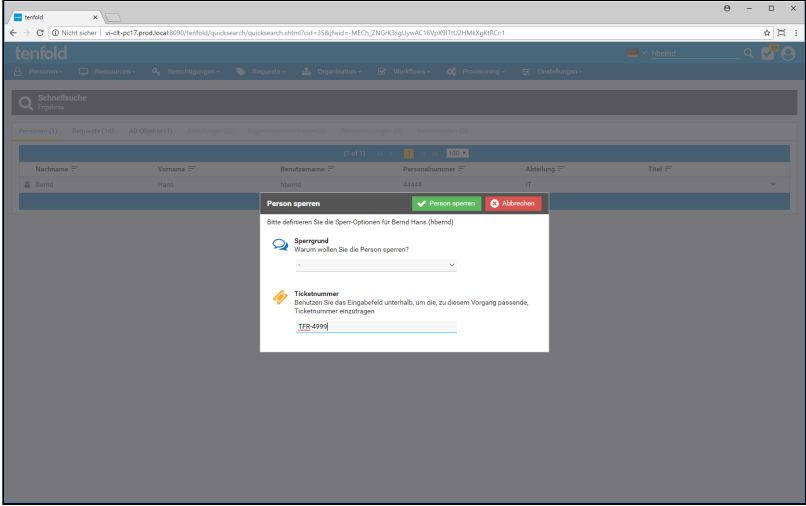
Auf dem Karteireiter "Allgemein" können eine Reihe von grundsätzlichen Einstellungen für die Personenart festgelegt werden.

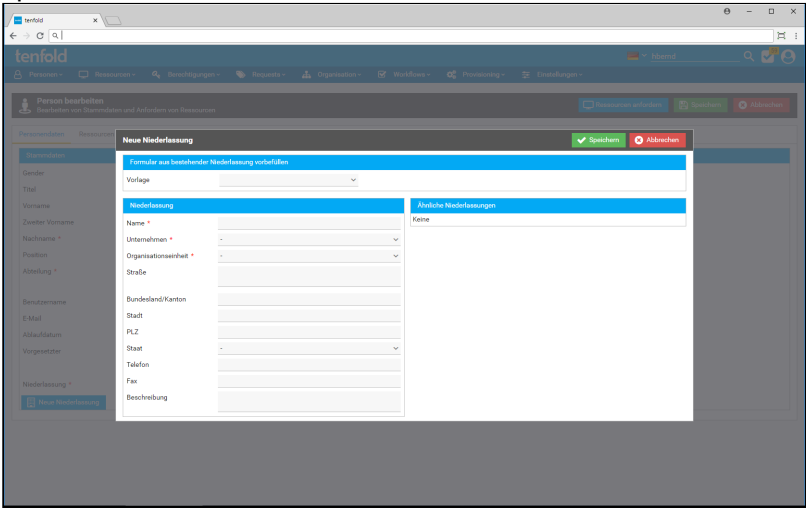
Abschnitt "Beschreibung"

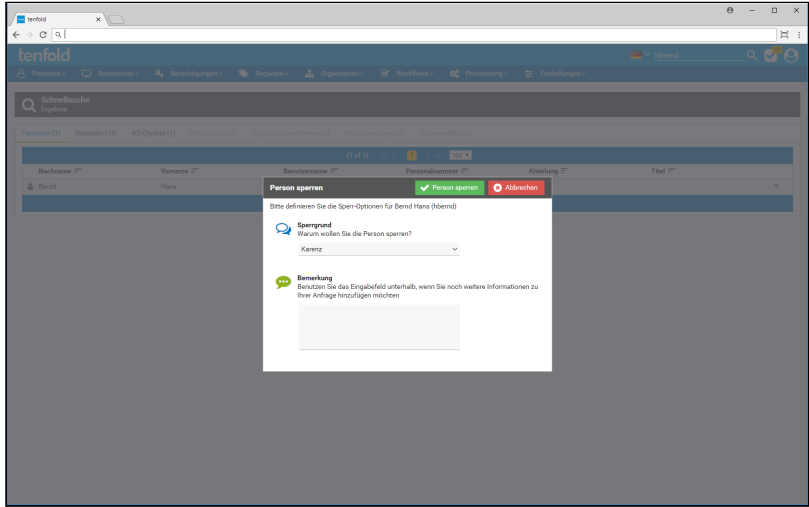
Einstellung	Beschreibung
Name	Der Name wird auf der Oberfläche verwendet, um die Personenart darzustellen.
Externe ID	Dient zur Synchronisierung mit Fremdsystemen (per Scripting) und wird in den meisten Fällen nicht benötigt
Personen-Icon	Das Personen-Icon legt das Symbol fest, welches in Personenlisten in der ersten Spalte angezeigt wird, um die Personenart darzustellen.
Beschreibung	In der Beschreibung kann der Anwendungsbereich dieser Personenart näher beschrieben werden. Dieser wird unter anderem auf der Self-Service-Oberfläche angezeigt.

Abschnitt "Allgemeine Optionen"

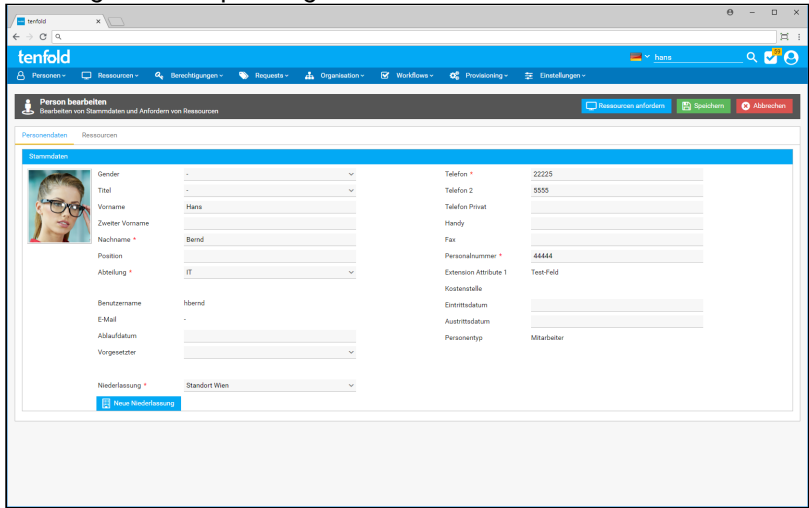
Einstellung	Beschreibung
Mehrere Niederlassungen	<p>Die Einstellung legt fest, ob dem Mitarbeiter genau eine Niederlassung zugeordnet werden kann oder ob dem Mitarbeiter mehrere Niederlassungen zugeordnet werden können, wovon eine als Hauptniederlassung fungiert. Je nach Konfiguration wird das entsprechende Eingabefeld als Auswahlliste oder als Mehrfachauswahl angezeigt, wenn eine Person angelegt oder bearbeitet wird. Das nachfolgende Beispiel zeigt die Maske mit aktivierten, mehrfachen Niederlassungen:</p> 

Einstellung	Beschreibung
Ticketnummer anzeigen	<p>Diese Option legt fest, ob beim Anlegen, Bearbeiten, Sperren, Entsperren, Verlängern oder Löschen einer Person dieser Art die Eingabe einer Ticketnummer möglich sein soll. Diese Funktion kann dazu genutzt werden, um im jeweiligen Request die Ticketnummer zu hinterlegen, mit dem die zugrundeliegende Anfrage in einem Helpdesk-System gespeichert wurde (zum Beispiel legt ein Abteilungsleiter ein Ticket an, um die IT anzuweisen, einen neuen Mitarbeiter anzulegen. Dieses Ticket erhält vom Ticketsystem eine Nummer, welche nun in tenfold hinterlegt werden kann, um nachträglich nachvollziehen zu können, aufgrund welches Tickets der Mitarbeiter angelegt wurde). Die Funktion dient somit primär dem Erhalt einer lückenlosen Dokumentation. Das folgende Beispiel zeigt die Möglichkeit der Ticketeingabe beim Sperren einer Person:</p> 

Einstellung	Beschreibung
<p>Niederlassungen anlegen erlaubt</p>	<p>Diese Einstellung legt fest, ob es möglich sein soll, für Personen dieser Art auf der Maske "Person bearbeiten" direkt über einen Button neue Niederlassungen anzulegen. Diese Option sollte genutzt werden, wenn Personen von Fremdfirmen in tenfold als eigene Personenart verwaltet werden. Dadurch können jene Unternehmen, für die diese Personen arbeiten, direkt bei der Anlage einer neuen Person mit angelegt werden. Ansonsten wäre es erforderlich, zuerst die Niederlassung anzulegen und diese dann bei der Person auszuwählen. Ein weiterer Vorteil besteht darin, dass für das Anlegen der Niederlassung keine gesonderte Berechtigungsprüfung stattfindet (Berechtigung "Manage Offices" - 8032). Somit können Benutzer, die üblicherweise keine Niederlassungen verwalten können, Niederlassungen über diesen Weg anlegen. Das folgende Beispiel zeigt den Dialog, der sich öffnet, wenn der Button "Neue Niederlassung" gedrückt wird, welcher durch Aktivieren dieser Option zusätzlich erscheint:</p> 
<p>Funktion Abteilungswechsel aktiv</p>	<p>Diese Einstellung legt fest, ob die Funktion "Abteilungswechsel" auf der Self-Service-Oberfläche für Personen dieser Personenart zur Verfügung stehen soll. Es handelt sich dabei um eine vereinfachte Variante zur Alternative, in der Maske "Person bearbeiten" das Feld "Abteilung" zu ändern.</p>

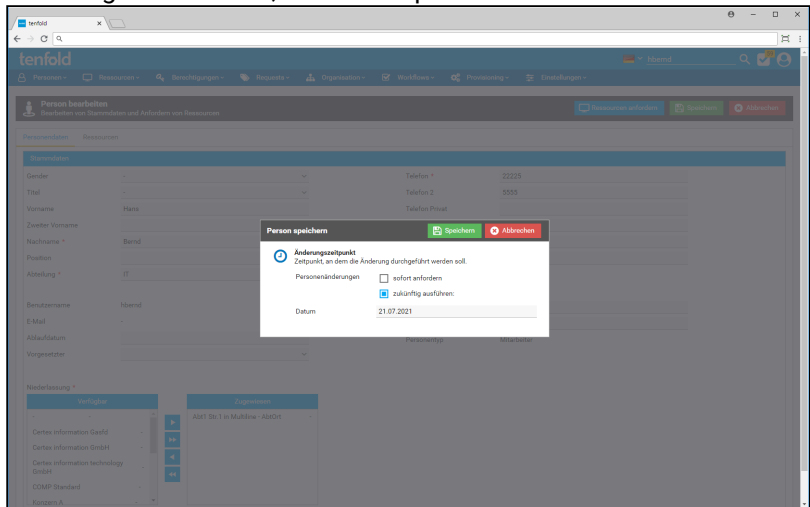
Einstellung	Beschreibung
Kommentar anzeigen	<p>Diese Option legt fest, ob bei Operationen die Person betreffend ein zusätzliches Kommentarfeld angezeigt werden soll. Dieses Feld kann für Notizen genutzt werden. Der Inhalt wird im Request gespeichert. Das folgende Beispiel zeigt dieses Kommentarfeld beim Sperren einer Person:</p> 

Abschnitt "Personenbilder"

Einstellung	Beschreibung
Personenbilder erlaubt	<p>Legt fest, ob auf der Maske "Person bearbeiten" bzw. "Person anzeigen" das Foto der Person angezeigt wird oder bearbeitet werden kann. Ist diese Option deaktiviert, wird nichts angezeigt. Ist die Option aktiviert, so wird im linken Bildschirmbereich das Foto angezeigt und alle Personenfelder werden entsprechend weiter rechts dargestellt. Das nachfolgende Beispiel zeigt die Maske mit aktiviertem Personenbild:</p> 

Einstellung	Beschreibung
Personenbilder erfordern Zustimmung	Mit dieser Option kann gesteuert werden, dass ein Benutzer, der ein Foto für seinen Personendatensatz hochladen möchte, zuerst eine Zustimmungserklärung bestätigen muss. In dieser Erklärung sollten Hinweise zum Datenschutz enthalten sein, die individuell je Organisation ausgestaltet sein müssen.
Zustimmungserklärung	Diese Einstellung ist nur aktiv, wenn Personenbilder eine Zustimmung erfordern. Die Erklärung muss als E-Mail-Vorlage hinterlegt werden. Diese Vorlage kann hier ausgewählt werden. Sie wird dem Benutzer vor dem Hochladen des Fotos angezeigt.

Abschnitt "Zukünftige Änderungen"

Einstellung	Beschreibung
<p>Bei Speichern von Personenänderung ermöglichen</p>	<p>Diese Einstellung legt fest, ob es erlaubt ist, Änderungen an einer Person erst zu einem späteren Zeitpunkt zu aktivieren. Sie können diese Einstellung auf "Nicht ermöglichen" setzen. Dies bewirkt, dass sämtliche Änderungen an Personen dieser Personenart sofort durchgeführt werden.</p> <p>Mit den anderen Einstellungen können auf der Maske "Person bearbeiten" zukünftige Änderungen erstellt werden. Mit diesen wird zum Zeitpunkt der Änderung selbst zwar ein Request erstellt, dieser verweilt allerdings im Status "Geplant", bis das eingegebene Aktivierungsdatum erreicht ist. Erst anschließend wird der Request ausgeführt. Diese Funktion kann beispielsweise dazu genutzt werden, um eine Stammdatenänderung an einer Person durchzuführen, die zwar heute schon bekannt ist, aber erst zu einem späteren Zeitpunkt aktiv werden soll. Gleich verhält es sich mit der Anlage von Personen: das Startdatum für den Mitarbeiter ist bereits bekannt und liegt in der Zukunft, die Eingabe soll allerdings schon jetzt erfolgen.</p> <p>Mit der Einstellung "Entscheidung bei Speichern ermöglichen (Legacy)" erscheint beim Speichern einer Person ein Dialog, mit welchem Sie auswählen können, ob die Änderung sofort oder zu einem späteren Zeitpunkt erfolgen soll. Das folgende Beispiel zeigt die Auswahl bei einer Änderung einer Person, wenn die Option aktiviert wurde:</p>  <p>Die Einstellung "Ermöglichen" zeigt die Schaltfläche "Neue zukünftige Änderung" an.</p>
<p>Ressourcen für zukünftige Stammdatenänderungen anfordern</p>	<p>Wenn diese Option aktiviert ist, so wirken die Berechtigungen für das Anfordern von Ressourcen auf der Self-Service-Oberfläche nicht nur auf Basis der aktuellen Stammdaten, sondern auch auf Basis der geplanten Änderung. Somit kann beispielsweise ein (geplanter) neuer Abteilungsleiter bereits vorab Ressourcen für Mitarbeiter bestellen, die in der Zukunft in seine Abteilung wechseln werden.</p>

Einstellung	Beschreibung
Durchführung	Diese Einstellung ermöglicht es zu entscheiden, ob Ressourcen-Requests, welche zu zukünftigen Personenänderungen bestellt wurden, direkt durchgeführt werden sollen oder erst gemeinsam mit der zukünftigen Personenänderung.
Zukünftige Änderungen der nächsten ... Tage anzeigen	Mit dieser Einstellung können Sie festlegen, wie viele Tage im voraus eine zukünftige Personenänderung in der Kachel "Zukünftige Änderungen" des Self-Service aufscheinen.

Abschnitt "Einstellungen"

Einstellung	Beschreibung
Niederlassungstypen	Diese Einstellung legt fest, welche Niederlassungen für Personen dieser Art gewählt werden können. Es stehen nur Niederlassungen zur Verfügung, die den ausgewählten Niederlassungstypen entsprechen. Diese Einstellung kann etwa dazu genutzt werden, um externe und interne Mitarbeiter zu trennen und jeweils nur die Auswahl von externen Firmen bei externen Mitarbeitern und von internen Niederlassungen bei internen Mitarbeitern zuzulassen.
Auswählbare Personenarten	Diese Option legt fest, in welche Personenart Personen dieser Art transformiert werden können. Einen Effekt hat diese Option nur dann, wenn das Feld "Personenart" in der Feldkonfiguration vorhanden und editierbar ist. Die Auswahl der verfügbaren Elemente in der Auswahlliste wird dann auf die hier definierten Einträge beschränkt.

Abschnitt "Personenanlage"

Die folgenden Optionen steuern den Ablauf und die verfügbaren Optionen bei der Anlage von neuen Personen. Alle nachfolgenden Optionen sind unter [Personen](#)(see page 63) detailliert beschrieben.

- Namenscheck anzeigen
- Benutzernamensvorschlag anzeigen
- Leeren User anlegen
- Person nach Profil anlegen
- Person mit zweiter Person als Vorlage anlegen
- Passwort vergeben
- Self-Service-Navigation

Abschnitt "Person sperren / entsperren / löschen (Zusammenfassung)"

Die Optionen in diesen drei Abschnitten koordinieren das Zusammenspiel zwischen Personen und den Ressourcen, die der Person zugeordnet wurden, im Falle von Sperren, Entsperren und Löschen. Die Operationen Sperren, Entsperren und Löschen können grundsätzlich auf zwei Ebenen durchgeführt werden: bei der Person selbst (zum Beispiel über das Kontextmenü im Ergebnis der Schnellsuche) und bei einer individuellen Ressourcenzuordnung der Person.

Die Option "Automatisch sperren/entsperren/löschen" legt dabei fest, dass die Person als Ganzes automatisch gesperrt/entsperrt/gelöscht wird, wenn:

- bereits alle, bis auf eine, Ressourcen gesperrt sind, die einem Benutzerkonto entsprechen (zum Beispiel eine Ressource für ein Active Directory-Konto) und nunmehr die letzte verbleibende Ressource auch gesperrt wird.
- bereits alle, bis auf eine, Ressourcen gesperrt sind nunmehr die letzte verbleibende Ressource auch gesperrt wird.
- Niemals

Workflow berücksichtigen

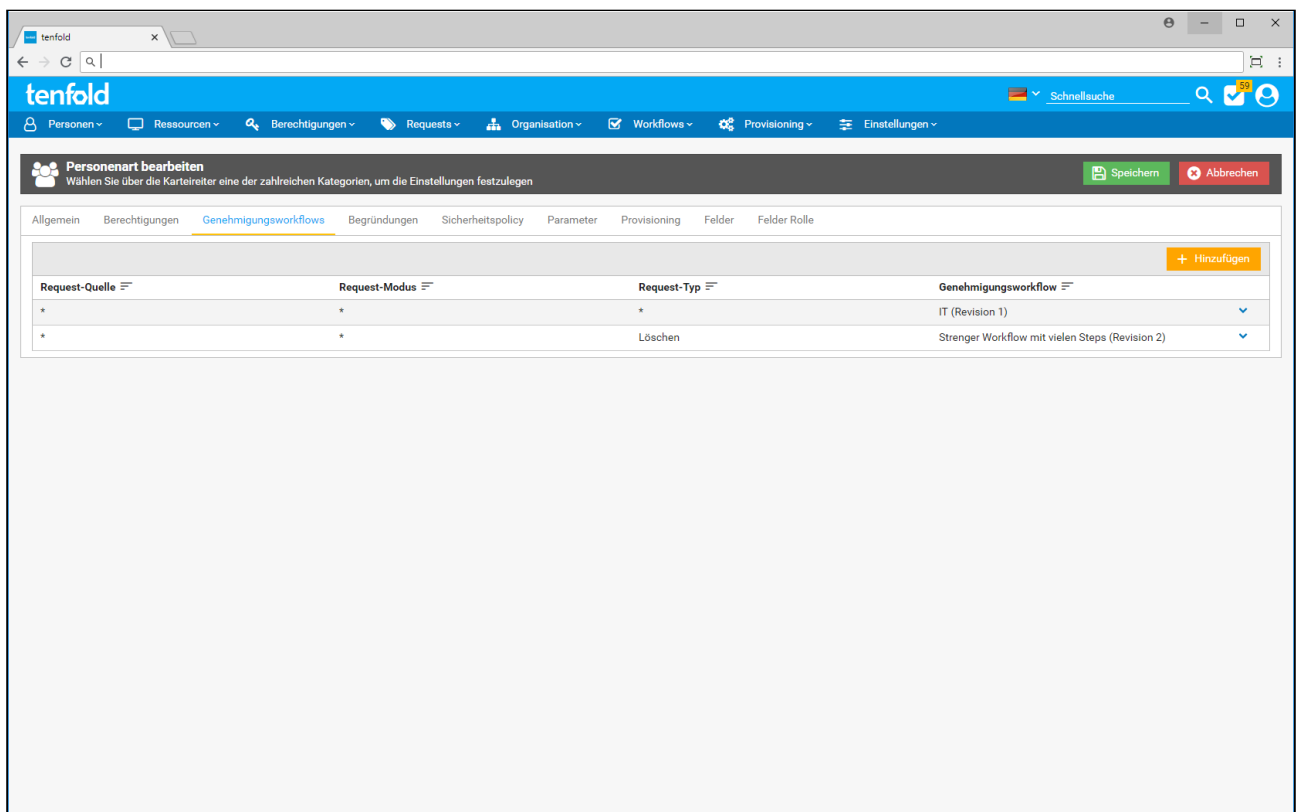
Die Sperre der Person erfolgt dabei nicht notwendigerweise im Handumdrehen. Es wird ein Request vom Typ "Sperre" für die Person angelegt. Dieser kann gegebenenfalls einem Genehmigungsworkflow unterliegen. Die Sperre wird erst dann ausgelöst, wenn der Workflow erfolgreich durchlaufen wurde.

Die Option "Ressourcenzuordnungen sperren/entsperren/löschen" bildet dabei den umgekehrten Weg ab. Sie legt fest, ob gegebenenfalls Requests zur Sperre/Entsperrung/Löschung der einzelnen Ressourcen angelegt werden sollen, wenn die Person als Ganzes gesperrt/entsperrt/gelöscht wird:

- Alle sperrbaren Ressourcen werden gesperrt (ob eine Ressource sperrbar ist - also auf den Request-Typ "Sperre" reagieren kann - wird in der Ressourcenkonfiguration festgelegt)
- Benutzerkonto-Ressourcen werden gesperrt
- Keine Ressourcen werden gesperrt

Genehmigungsworkflows

Auf diesem Karteireiter wird festgelegt, welche Genehmigungsworkflows für die unterschiedlichen Operationen an Personen dieser Personenart gelten sollen. Es kann nicht nur ein globaler Workflow hinterlegt werden, sondern es kann danach unterschieden werden, aus welcher Request-Quelle der entsprechende Request stammt (zum Beispiel "tenfold" bei einer manuellen Anlage über die Oberfläche oder "Extern" im Falle einer Anlage durch einen Import aus einem externen System) und welche Operation durchgeführt werden soll (Request-Typ). Wie bei jeder Entscheidungstabelle steht der Wert "*" für jeden beliebigen Wert. In folgendem Beispiel werden etwa alle Änderungen grundsätzlich mit dem Workflow "IT" behandelt. Nur beim Löschen von Personen kommt ein anderer, strengerer Workflow zum Tragen:



Achtung

In dieser Entscheidungstabelle zählt nicht - wie üblich - die Reihenfolge, sondern es wird der Eintrag ausgewählt, der am besten passt (gemessen an der Anzahl der zutreffenden Merkmale). Treffen bei mehreren Einträgen mehrere Merkmale zu, ist die Verarbeitungsreihenfolge nicht definiert. Es wird somit empfohlen, die Definitionen möglichst genau vorzunehmen, um Unklarheiten zu vermeiden.

Passwort-Reset

Im Karteireiter "Passwort-Reset" werden die Einstellungen für den Passwort-Reset getroffen. Die Einstellungen betreffen sowohl den Passwort-Reset über die tenfold Weboberfläche als auch den Reset über das Self-Service-Passwort-Reset-Portal.

Folgende Einstellungen können hierbei vorgenommen werden:

Einstellung	Beschreibung
Passwortrichtlinie	Legt fest, welcher Richtlinie das gewählte Passwort entsprechen muss. Die Richtlinien werden im Menü unter <i>Einstellungen > Richtlinien > Passwortrichtlinien</i> konfiguriert.
Verifizierungsrichtlinie	Die Verifizierungsrichtlinie legt fest, wie sich der Benutzer gegenüber tenfold verifizieren kann. Mögliche Optionen sind One-Time-Passwords oder Geheimantworten. Die Richtlinien werden im Menü unter <i>Einstellungen > Richtlinien > Verifizierungsrichtlinien</i> konfiguriert.

Einstellung	Beschreibung
Password-Reset-Scope	<p>Es kann festgelegt werden, auf welcher Ebene die Passwörter anschließend gesetzt werden. Mögliche Einstellungen sind:</p> <ul style="list-style-type: none"> • Alle Ressourcenzuordnungen mit Passwortänderung: Es werden die Passwörter aller Ressourcenzuordnungen auf dasselbe Passwort gesetzt. Eine Auswahl über einzelne Zuordnungen ist nicht möglich. • Ressourcenzuordnungen auswählen: Es kann beim Zurücksetzen ausgewählt werden, für welche Ressourcenzuordnungen die Passwörter zurückgesetzt werden. Für alle ausgewählten Zuordnungen wird hierbei dasselbe Passwort gesetzt. <p>Achtung: Passwörter können nur für Zuordnungen zurückgesetzt werden, bei deren Ressource die Einstellung "Passwortänderung möglich" aktiviert wurde. (Siehe Ressourcenverwaltung(see page 125))</p>
Berechtigung eigenes	Definiert, welche Berechtigung zugeordnet sein muss, damit man sein eigenes Passwort zurücksetzen kann.
Berechtigung fremdes	Definiert, welche Berechtigung zugeordnet sein muss, damit man das Passwort einer anderen Person zurücksetzen kann.
Eingabemodus eigenes	Legt fest, ob beim Zurücksetzen des eigenen Passworts entweder automatisch ein Passwort generiert wird oder ob das Passwort eingegeben werden kann.
Eingabemodus fremdes	Legt fest, ob beim Zurücksetzen des Passworts einer anderen Person entweder automatisch ein Passwort generiert wird oder ob das Passwort vom Benutzer eingegeben werden kann.
Eingabemodus Passwortportal	Legt fest, ob beim Zurücksetzen des eigenen Passworts über das Self-Service-Password-Reset-Portal automatisch ein Passwort generiert wird, oder ob das Passwort vom Benutzer eingegeben werden kann.
Verifizierungsrichtlinie (2)	<p>Diese Richtlinie kommt zum Tragen, wenn der Benutzer die Antworten auf seine Sicherheitsfragen festlegen möchte. Selbst wenn der Benutzer ordnungsgemäß bei tenfold angemeldet ist, muss er sich deshalb über diese Richtlinie verifizieren, damit ausgeschlossen werden kann, dass zum Beispiel ein Dritter einen nicht gesperrten PC übernimmt und durch Festlegen der Sicherheitsfragen und Antworten das Passwort des angemeldeten Benutzers zurücksetzen und sich damit die Herrschaft über das Konto sichern kann.</p> <p>Die hinterlegte Richtlinie könnte zum Beispiel eine erneute Eingabe des Active Directory-Passworts erfordern.</p>

Parameter

Nur für Experten

Die Einträge in dieser Tabelle dienen dazu Werte festzulegen, die anschließend über das interne Scripting, im Rahmen des Groovy Plugin, abgefragt werden können. Neue Einträge können mit dem "Hinzufügen"-Button hinterlegt werden. Bestehende Einträge können sowohl bearbeitet als auch gelöscht werden.

Provisioning

Mit dem Provisioning ist es möglich, bei bestimmten Ereignissen, welche die Person betreffen, ein Plugin zu nutzen. Neue Provisionierungsschritte können hinzugefügt werden (Button "Provisionierungsschritt hinzufügen"), bestehende Schritte können angepasst (Button "Bearbeiten") oder gelöscht werden (Button "Löschen"). Zusätzlich kann gesteuert werden, dass ein Schritt nur unter bestimmten Voraussetzungen ausgeführt wird (siehe Button "Bedingungen" sowie [Bedingungen](#)(see page 578)).

Die einzelnen Einstellungen pro Schritt sind abhängig davon, welches Plugin zum Einsatz kommt. Die Konfigurationsmöglichkeiten sind in der Beschreibung des jeweiligen Plugins zu finden.

Felder

Im Karteireiter "Felder" wird konfiguriert, welche Attribute zu Personen der jeweiligen Personenart gespeichert werden sollen. Es ist dabei zu berücksichtigen, dass es sich hierbei um Attribute (Felder) handelt, die in der tenfold-Datenbank gespeichert werden. Die Feldkonfiguration einer Personenart trifft alleine noch keine Aussage darüber, wie diese Felder anschließend in angebundene Fremdsysteme übertragen werden (beispielsweise, welche Active Directory-Attribute mit diesen Feldinhalten aus tenfold verknüpft werden). Dafür ist das Feldmapping verantwortlich, welches im Plugin für das betroffene Zielsystem eingestellt werden muss.

Der Maskenaufbau bildet dabei den Aufbau der Stammdatenansicht für Personen dieser Art ab. Er besteht aus drei Bereichen:

- Linke Spalte der Stammdatenmaske
- Rechte Spalte der Stammdatenmaske
- Feldauswahlbereich

Die einzelnen Felder werden dabei farblich unterschiedlich dargestellt: Rote Felder sind Pflichtfelder, blaue sind optionale Felder. Pflichtfelder müssen einen Wert haben, bevor die Daten gespeichert werden können, blaue Felder dürfen leer bleiben. Das Icon in der Titelzeile des jeweiligen Feldes zeigt dabei den Datentyp des Feldes an:

- Stift: Textfeld
- Pfeil nach unten: Auswahlfeld
- Kalender: Datum
- Häkchen: Auswahlfeld (Checkbox)

Darüber hinaus werden einige Eigenschaften der Felder bereits in der Übersicht durch Icons dargestellt:

- Rufzeichen: Erforderliches Feld
- A-Symbol: Es ist eine Übersetzung für das Feld vorhanden
- X-Symbol: Das Feld wird im Export verwendet
- Häkchen: Für das Feld ist eine Validierungsregel hinterlegt.

Im obigen Beispiel stellt der Vorname das erste Feld der linken Spalte und die Telefonnummer das erste Feld der rechten Spalte dar. Auf der Maske "Person bearbeiten" wird dies wie folgt dargestellt:

Person bearbeiten (Reimann Walter)
Bearbeiten von Stammdaten und Anfordern von Ressourcen

Personen

Personendaten Ressourcen Lifecycle (Aktiv)

Stammdaten

Vorname * Telefon

Zweiter Vorname Telefon 2

Nachname * Telefon Privat

Position Handy

Abteilung * Fax

Benutzername Personalnummer

Email Kostenstelle

Ablaufdatum Personenart

Vorgesetzter

Standort *

Liste der Felder

Folgende Felder stehen für die Konfiguration zur Verfügung:

Name	Datentyp	Beschreibung
BUILDING	Gebäude Menü: Organisation > Gebäude	Auswahl des Gebäudes, in dem sich das Büro der Person befindet
CHECK1-5	Checkbox / Boolean	Benutzerdefinierte Auswahlfelder (Checkboxes)
COST_CENTER	Kostenstelle Menü: Organisation > Kostenstellen	Auswahl der Kostenstelle, der die Person zugeordnet ist
DATE1-5	Datum / Kalenderauswahl	Benutzerdefinierte Datumsfelder (Auswahl über Kalender)
DEPARTMENT	Abteilung Menü: Organisation > Abteilungen	Auswahl der Abteilung der Person. Dieses Feld ist für jede Personenart verpflichtend.

Name	Datentyp	Beschreibung
EID	Zeichenkette	Kann genutzt werden, um einen Externen Identifier für diese Person zu hinterlegen. Dieses Feld wird nur beim Import von Personendaten aus vorgelagerten Systemen genutzt.
EMAIL	Zeichenkette	E-Mail-Adresse der Person. Sofern die Adresse von einem Plugin generiert wird, sollte das Feld nicht editierbar konfiguriert werden.
EMPLOYEE_ID	Zeichenkette	Personalnummer
EXPIRE	Datum	Ablaufdatum der Person
FAX	Zeichenkette	Faxnummer
FAX2	Zeichenkette	Alternative Faxnummer
FIRST_NAME	Zeichenkette	Vorname
FIRST_NAME2	Zeichenkette	Zweiter Vorname
GENDER	Geschlecht Menü: Personen > Stammdaten > Gender	Auswahl des Geschlechts der Person
IDENTITY_TYPE	Personenart Menü: Personen > Stammdaten > Personenarten	Personenart der Person
INFO1-15	Zeichenkette	Benutzerdefinierte Textfelder
IT_COST_CENTER	Kostenstelle Menü: Organisation > Kostenstellen	Gegebenenfalls abweichende IT-Kostenstelle
JOB_TITLE	Zeichenkette	Positionsbeschreibung als Freitext. Alternativ kann die Position auch als Auswahlliste gestaltet werden, siehe Feld "POSITION".
JOINING_DATE	Datum	Eintrittsdatum
LANGUAGE	Sprache Einstellungen > Sprachen	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>
LAST_NAME	Zeichenkette	Nachname

Name	Datentyp	Beschreibung
LAST_NAME2	Zeichenkette	Zweiter Nachname
LEAVING_DATE	Datum	Austrittsdatum
MIDDLE_NAME	Zeichenkette	Mittlerer Name
MIDDLE_NAME2	Zeichenkette	Zweiter mittlerer Name
MOBILE	Zeichenkette	Mobilnummer
OFFICE	Niederlassung Menü: Organisation > Niederlassungen	Niederlassung des Mitarbeiters. Wenn in den Einstellungen der Personenart "Mehrere Niederlassungen" konfiguriert ist, so handelt es sich um eine Mehrfachauswahl.
OFFICE2	Niederlassung	Zweite Niederlassung des Mitarbeiters. Kann genutzt werden, wenn exakt zwei Niederlassungen gespeichert werden können sollen. Sollen eine oder beliebig viele Niederlassungen gespeichert werden sollen, so sollte das Feld "OFFICE" in Verbindung mit der Einstellung "mehrere Niederlassungen" verwendet werden.
OFFICE_CODE	Zeichenkette	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>
PERSON1-5	Person	Benutzerdefinierte Auswahl einer anderen Person (zum Beispiel, um einen internen Ansprechpartner für eine externe Person abzubilden)
PERSONAL_FAX	Checkbox	Kennzeichen, ob es sich beim Feld "FAX" um eine persönliche Faxdurchwahl handelt.
PERSON_TITLE	Titel Menü: Personen > Stammdaten > Titel	Titel der Person
PHONE	Zeichenkette	Telefonnummer
PHONE2	Zeichenkette	Zweite Telefonnummer
PHONE_HOME	Zeichenkette	Private Telefonnummer
POSITION	Position Menü: Personen > Stammdaten > Positionen	Berufliche Position als Auswahlliste (alternativ kann diese Angabe auch als Zeichenkette erfolgen, wenn das Feld "JOB_TITLE" verwendet wird).

Name	Datentyp	Beschreibung
POST_NAME_TITLE	Titel Menü: Personen > Stammdaten > Titel	Titel nach Name (zum Beispiel "Ph.D.")
PRE_NAME_TITLE	Titel Menü: Personen > Stammdaten > Titel	Titel vor Name (zum Beispiel "Dr.")
Platzhalter	Platzhalter	Wenn der Platzhalter genutzt wird, bleibt die gewählte Spalte in der jeweiligen Zeile frei. So kann die Stammdatenansicht, zum Beispiel mit Leerzeilen, übersichtlicher gestaltet werden.
REGION	-	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>
REQUEST_REASON	-	<i>Es handelt sich um eine Legacy-Einstellung, die nicht mehr verwendet werden sollte.</i>
ROOM_NUMBER	Freitext	Raumnummer
SUPERIOR	Person	Direkter Vorgesetzter
USER_PRINCIPAL_NAME	Zeichenkette	Der UPN des Active Directory Benutzers. Dieses Feld wird in Verbindung mit dem tenfold Office 365 Lifecycle Plugin und dem tenfold Mailbox Lifecycle Plugin für Exchange Online benötigt.
VALUE_GROUP1-5	Nachschlagewert Menü: Einstellungen > Nachschlagewerte	Benutzerdefinierte Auswahl eines Werts aus einer vorgegebenen Liste von möglichen Werten.

Felder bearbeiten

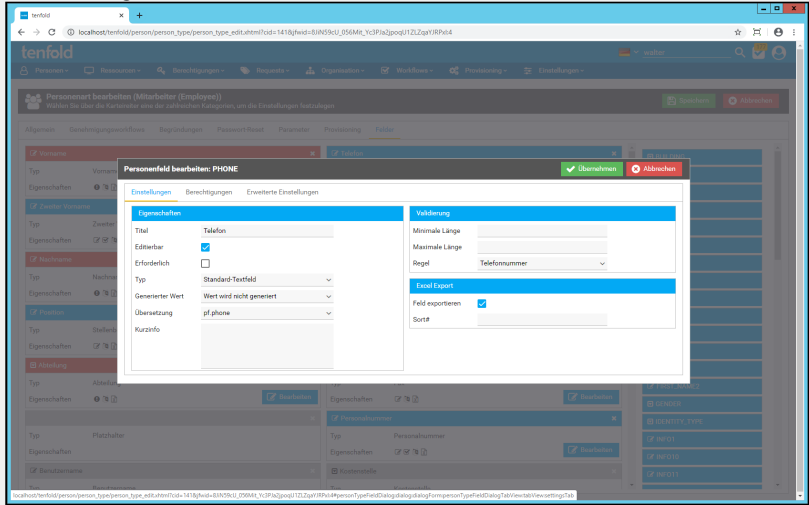
Um Felder für die Personenart zu bearbeiten oder die Anordnung der linken oder rechten Spalte zu ändern, nutzen Sie Drag & Drop:

- Ziehen Sie Felder aus dem rechten Bereich in die linke oder rechte Spalte, um diese hinzuzufügen
- Ziehen Sie Felder, die sich bereits in der linken oder rechten Spalte befinden, an die gewünschte Position (nutzen Sie zum "Drag" dabei die Titelleiste des jeweiligen Feldes)
- Entfernen Sie ein Feld, in dem Sie das Löschen-Icon drücken, welches sich rechts in der Titelleiste des jeweiligen Feldes befindet

Details bearbeiten / Eigenschaften

Für jedes Feld können Detailinformationen bearbeitet werden. Folgende Einstellungen können in den Karteireitern "Einstellungen", "Berechtigungen" und "Erweiterte Einstellungen" getroffen werden:

Einstellung	Beschreibung
-------------	--------------

	
<p>Titel</p>	<p>Legt fest, wie das Feld auf der Stammdatenansicht einer Person bezeichnet werden soll. Diese Einstellung greift nur, wenn keine Übersetzung definiert wurde oder keine passende Übersetzung gefunden wurde.</p>
<p>Editierbar</p>	<p>Definiert, dass das Feld editierbar ist. Ist diese Option nicht aktiviert, so wird das Feld zwar angezeigt, kann aber nicht bearbeitet werden. Siehe auch Karteireiter "Berechtigungen", wie diese Einstellung außer Kraft gesetzt werden kann.</p>
<p>Erforderlich</p>	<p>Diese Option legt fest, dass für dieses Feld ein Wert eingegeben/ausgewählt werden muss. Siehe auch Karteireiter "Berechtigungen", wie diese Einstellung außer Kraft gesetzt werden kann.</p>
<p>Filter</p>	<p>Diese Option ist nur für Auswahlfelder verfügbar. Sie legt fest, ob die Liste zur Auswahl eines Wertes auch über einen Textfilter verfügen soll.</p>
<p>Generierter Wert</p>	<p>Soll das Personenfeld mit einem generierten Wert befüllt werden, so kann er an dieser Stelle ausgewählt werden. Mehr dazu unter Generierte Werte (see page 603).</p>
<p>Übersetzung</p>	<p>Es kann ein Übersetzsungs-Tag definiert werden, der genutzt wird, um die Bezeichnung mehrsprachig darzustellen. Wenn keine Übersetzung hinterlegt ist, oder für die ausgewählte Sprache keine Übersetzung für den Tag vorhanden ist, wird der Titel zur Anzeige verwendet.</p>
<p>Kurzinfo</p>	<p>Es kann hier ein Kurztext hinterlegt werden, welcher anschließend über einen Tooltip neben dem Feld auf der Stammdatenansicht sichtbar wird. Hier können zum Beispiel Hinweise zum gewünschten Eingabeformat hinterlegt werden.</p>
<p>Minimale Länge</p>	<p>Bei Textfeldern kann festgelegt werden, wie viele Zeichen das Feld mindestens umfassen muss.</p>

Maximale Länge	Bei Textfeldern kann festgelegt werden, wie viele Zeichen das Feld maximal umfassen darf.
Regel	<p>Für Textfelder kann hier eine Validierungsregel ausgewählt werden:</p> <ul style="list-style-type: none"> • No Rule: Es kommt keine Validierungsregel zur Anwendung • Regular Expression: Validierung über einen regulären Ausdruck (siehe https://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html) • Code Snippet: Validierung über ein Code Snippet (siehe den Hinweis zur Verwendung unterhalb) • Vordefinierte: Es existieren eine Reihe von vordefinierten Regeln für Telefonnummern, URLs und andere.
Prüfung auf Eindeutigkeit - Aktiv	Ist diese Einstellung ausgewählt, wird vor dem Speichern auf die Eindeutigkeit des Feldinhaltes geprüft. Dies bedeutet, dass eine Person nur dann gespeichert werden kann, wenn der Inhalt dieses Feldes nicht bereits bei einer anderen Person in diesem Feld vorhanden ist.
Prüfung auf Eindeutigkeit - Anwenden auf	<p>Ist die Einstellung "Prüfung auf Eindeutigkeit" aktiv, so kann mit dieser Einstellung eingeschränkt werden, welche Personen in die Eindeutigkeitsprüfung mit einbezogen werden. Folgende Auswahlmöglichkeiten stehen zur Verfügung:</p> <ul style="list-style-type: none"> • Alle Personen: Das Feld muss über alle im System vorhandenen Personen eindeutig sein. • Personen derselben Personenart: Das Feld muss über alle Personen mit der selben Personenart, wie die der bearbeiteten Person, eindeutig sein. • Feldregeln: Es können Feldregeln ausgewählt werden und das Feld muss eindeutig zwischen all den Personen sein, auf welche die ausgewählten Feldregeln zutreffen.
Feld exportieren	Definiert, ob dieses Feld beim Export eines Suchresultats in der Exportdatei enthalten sein soll (siehe dazu auch Personensuche (see page 357)).
Sort#	Legt die Reihenfolge der Felder (entspricht den Spalten) in der Exportdatei fest. Wenn keine Sortierreihenfolge festgelegt ist, definiert die Datenbank die Reihenfolge (diese ist somit nicht vorhersehbar).