




















EXEC "ResetPassword.validatePolicy" verwenden	In älteren Installationen von tenfold wurde die Überprüfung der Verifizierungsrichtlinie verwendet. Mit dieser werden Personen zur Rücksetzung des Passwortes authentifiziert ohne das Passwort zu kennen. In neueren Installationen von tenfold wird dies allein durch die Einstellungen in der Verifizierungsrichtlinie gesteuert. Sollten Sie von älteren Installationen von tenfold diesen EXEC angepasst haben um die Verifizierung durchzuführen, aktivieren Sie diesen Parameter um Ihre Anpassungen weiterhin zu verwenden. Hinweis: In neueren Installationen von tenfold wird nicht empfohlen diese Einstellung zu aktivieren.	Checkbox	
Generiertes Passwort anzeigen	Ist diese Einstellung aktiv, können beim Zurücksetzen von Passwörtern, generierte Passwörter angezeigt werden.	Checkbox	
> Personen-Lifecycle			
Ablaufende Personen - Ausgenommen Lifecycle-Phasen	Auf der Maske "Ablaufende Personen und "Ablaufende Ressourcenzuordnungen" werden jene Personen angezeigt, welche in der kommenden Zeit ablaufen oder bereits abgelaufen sind. Diese Auflistung kann jedoch sehr unübersichtlich werden, wenn zum Beispiel ausgetretene Mitarbeiter nicht gelöscht werden und diese sich dann für immer in dieser Auflistung befinden. Zu diesem Zweck kann in diesem Feld eine kommagetrennte Liste mit IDs von Lifecycle-Phasen aufgeführt werden. Personen und deren Ressourcenzuordnungen werden dann in diesen Auflistungen nicht aufgeführt, wenn Sie sich in einer der angegebenen Lifecycle-Phasen befinden.	Text	
Gesperrte Personen - Ausgenommene Lifecycle-Phasen	Diese Einstellung verhält sich analog zu "Ablaufende Personen - Ausgenommen Lifecycle-Phasen" für die Masken "Gesperrte Personen" und "Gesperrte Ressourcenzuordnungen.	Text	
Ursprünglichen Anforderer für Requests verwenden	Legt fest, ob der Anforderer, welcher den Lifecycle-Wechsel angefordert hat, verwendet werden soll, als Anforderer für alle entstehenden untergeordneten Requests. Andernfalls wird der tenfold Systembenutzer (systemfold) verwendet. Hinweis: Dies kann eine Auswirkung haben, wenn Genehmigungsworkflows hinterlegt wurden und der ursprüngliche Anforderer nicht über alle Berechtigungen verfügt.	Checkbox	

Ursprünglichen Anforderer für Requests von Job verwenden		Checkbox	
> Personen-Verknüpfungen			
Ursprünglichen Anforderer für Requests verwenden	Legt fest, ob der Anforderer, welcher die Personenänderung beantragt hat, auch für die Änderungs-Requests der verknüpften Personen verwendet werden soll. Falls nicht, wird stattdessen der Systembenutzer (systemfold) verwendet.	Checkbox	
> Plugins			
Plugin-Informationen aus dem Internet abrufen	Legt fest, ob neue oder aktualisierte Plugins aus dem Internet heruntergeladen werden können. Ist diese Einstellung deaktiviert, können Plugins nur aus dem Verzeichnis "<tenfold-Installationsverzeichnis>\plugins" heraus installiert werden. Sollte der Rechner auf welchem tenfold installiert ist, keinen Zugriff auf das Internet haben, kann das Deaktivieren dieser Einstellung den Aufruf der Plugin-Verwaltungsmaske (Provisioning > Plugins > Verwaltung) beschleunigen.	Checkbox	
Upload-Button sichtbar	Steuert die Sichtbarkeit des Buttons zum Upload von Plugins auf der Plugin-Verwaltungsmaske. Verwenden Sie diese Einstellung nur, falls Plugins speziell für Sie entwickelt wurden, welche nicht im tenfold-Marketplace verfügbar sind und Sie keinen direkten Zugriff auf den tenfold-Server haben. Sollten Sie Zugriff auf den tenfold-Server haben, wird empfohlen stattdessen die Plugins im Verzeichnis "<tenfold-Installationsverzeichnis>\plugins" abzulegen.	Checkbox	
URL zu Plugin-Informationen	Legt den URL fest, unter welchem tenfold nach Informationen zu aktualisierten Plugins sucht. Dieser URL muss mit https:// (Internet) oder file:// (lokale Datei) beginnen. Ist dieser Systemparameter leer, verwendet tenfold den üblichen tenfold-Marketplace. Achtung: Normalerweise besteht kein Bedarf, diese Einstellung zu ändern. Ändern Sie diesen Systemparameter nur wenn es durch spezielle Anforderungen notwendig ist und klären Sie die Einstellung mit Ihrem tenfold-Partner. Sollten Sie diese Einstellung ändern, kann tenfold keine Plugins mehr aus dem standard tenfold-Marketplace beziehen.	Text	

> Profile			
Abgleich - Inaktive Active Directory-Objekte	Diese Einstellung legt fest, ob beim Abgleich von Profilinhalten, deaktivierte Active Directory-Objekte berücksichtigt werden. Ist diese Einstellung deaktiviert, werden inaktiven Benutzerkonten keine Gruppen durch Profilzuordnungen zugewiesen.	Checkbox	
Abgleich - Requests automatisch genehmigen	Dieser Systemparameter bestimmt, ob Requests die durch den automatischen Profilabgleich einer Person entstehen, automatisch genehmigt werden oder nicht.	Checkbox	
Ursprünglichen Anforderer für Requests verwenden	Legt fest, ob bei der Erstellung von Requests durch die Zuweisung eines Profils, der ursprüngliche Anforderer, welcher die Zuordnung des Profils angefordert hat, verwendet werden soll oder nicht. Falls nicht, wird der Systembenutzer (systemfold) verwendet.	Checkbox	
Ursprünglichen Anforderer für Requests von Job verwenden	Wenn beim Ablauf einer Profilzuordnung Requests erstellt werden, wird standardmäßig der tenfold Systembenutzer als Anforderer für alle Requests verwendet. Ist diese Einstellung aktiv, wird stattdessen jene Person verwendet, welche den Ablauf der Zuordnung beantragt hat.	Checkbox	
> Provisionierung			
EXECs in Logdatei ausgeben	Mit diesem Systemparameter wird bestimmt, ob bei der Durchführung der Provisionierungen ausgeführte EXECs, in der Log-Datei ausgegeben werden sollen oder nicht. Werden die EXECs nicht ausgegeben, kann das den Umfang Ihrer Log-Datei erheblich verringern. Es erschwert jedoch auch die Analyse von Problemen durch den Produktsupport.	Checkbox	
> REST API			



Authentifizierungsversuche - Authentifizierung deaktiviert	<p>Nach einer gewissen Anzahl fehlgeschlagener Versuche (3, 5, 10 und 20) sich an dem Rest-API mittels eines gültigen API-Keys anzumelden, wird die IP von welcher die Anmeldeversuche ausgegangen sind, für eine gewisse Zeit gesperrt und kann in dieser Zeit keine weiteren Versuche durchführen. Mit dieser Einstellung können Sie festlegen, wie lange die Zeit ist, in welcher Anmeldeversuche blockiert werden. Die Zeiten sind in Sekunden angegeben und durch Komma (,) zu trennen. Achtung: Es dürfen keine Leerzeichen enthalten sein.</p> <p>Beispiel: Mit der Standardeinstellung "30,300,600,3600", ist nach der ersten und zweiten fehlgeschlagenen Anmeldung sofort ein weiterer Anmeldeversuch möglich. Danach werden weitere Anmeldeversuche jeweils 30 Sekunden blockiert. Nach der insgesamt fünften fehlgeschlagenen Anmeldung wird diese Zeit auf 5 Minuten (300 Sekunden erhöht). Nach dem insgesamt 10. fehlgeschlagenen Anmeldeversuch erhöht sich die Zeit der Blockierung auf 10 Minuten (600 Sekunden) und nach der 20. fehlgeschlagenen Anmeldung auf eine Stunde (3600 Sekunden).</p>	Text	
> Self-service			
Beschreibung durchsuchen	Wenn Sie bei der Bestellung von Ressourcen im Self-Service die Suche für Ressourcen verwenden, wird standardmäßig nur der Name der Ressourcen für die Suche herangezogen. Ist diese Einstellung aktiviert, wird auch die Beschreibung der Ressourcen herangezogen.	Checkbox	
Fileserver-Anforderungsmodus	Mit dieser Einstellung können Sie festlegen, ob im Self-Service für Fileserver-Berechtigungen pro Bestellung nur eine Berechtigung bestellt werden kann oder ob mehrere Berechtigungen in einer Anforderung bestellt werden können.	Auswahl	
Maximal anzuzeigende Personen	Sollte eine Person in tenfold für sehr viele Personen die Berechtigung zur Anforderung haben, kann das Laden für die Maske zur Auswahl der Person im Self-Service eine gewisse Zeit in Anspruch nehmen. Um dies einzudämmen wird ab einer gewissen Anzahl von Personen nur mehr eine Information angezeigt, dass zu viele Personen gefunden wurden und das Suchfeld zum Ausfindigmachen der gewünschten Person verwendet werden muss. Mit dieser Einstellung können Sie festlegen, ab wie vielen Personen dies der Fall ist.	Text	




Meine Requests - Ticketnummer anzeigen	Mit dieser Einstellung legen Sie fest, ob auf der Maske "Meine Requests" eine Spalte für die Ticketnummern der Requests eingeblendet wird.	Checkbox	✗
Personen-Cache - Aktiv	Mit dieser Einstellungen können Sie bestimmen, ob die zur Auswahl stehenden Personen im Self-Service gecached werden oder jedes mal neu geladen werden sollen. Achtung: Deaktivieren Sie diese Einstellung nicht ohne vorher durch den Support dazu aufgefordert zu werden.	Checkbox	✗
> SharePoint			
SharePoint-Berechtigungen bearbeiten - Kommentar anzeigen	Legt fest, ob bei der Bestellung von SharePoint-Berechtigungen ein Kommentar für den Request eingegeben werden kann.	Checkbox	✗
SharePoint-Berechtigungen bearbeiten - Kommentar erforderlich	Bestimmt, ob ein Kommentar für die Bestellung von SharePoint-Berechtigungen verpflichtend ist.	Checkbox	✗
> Stellvertretungen			
Berechtigungsvererbung - Aktiv	Stellvertreter erhalten alle tenfold-Berechtigungen der Person welche Sie vertreten (siehe Stellvertretungen (see page 372)). Ist diese Einstellung aktiv, erhalten Stellvertreter nicht nur die Berechtigungen der Person welche Sie stellvertreten, sondern auch sämtliche Berechtigungen welche die stellvertretene Person als Stellvertreter von anderen Personen erhält. Es gibt keine Begrenzung über wie viele Ebenen Berechtigungen vererbt werden. Mit dieser Einstellung können keine zyklischen Stellvertretungen definiert werden. Eine Vertretung A > B > C > A ist daher nicht möglich. Ist diese Einstellung deaktiviert, findet keine Vererbung von Stellvertreter-Berechtigungen mehr statt. Dies bedeutet, dass man nur mehr exakt jene Berechtigungen als Stellvertreter erhält, welche die stellvertretene Person direkt zugeordnet hat, ohne Berücksichtigung weiterer Stellvertretungen. Mit dieser Einstellung lassen sich zyklische Vertretungen A > B > C > A definieren. Warnung: Sollten zyklische Stellvertretungen existieren, wenn Sie diese Einstellung aktivieren, kann dies zu Problemen bei der Anmeldung von Benutzern führen. Es findet keine Prüfung auf die Existenz solcher Stellvertretungen statt.	Checkbox	✗

> Sucheinstellungen und Suchergebnisse			
Zeilen Pro Seite	Legt fest, wie viele Tabellenzeilen pro Seite in Suchergebnissen angezeigt wird.	Text	✗
>> Personensuche			
Abteilung anzeigen	Legt fest, ob in den Resultaten von Personensuchen eine Spalte für die Abteilung angezeigt wird.	Checkbox	✗
E-Mail anzeigen	Legt fest, ob in den Resultaten von Personensuchen eine Spalte für die E-Mail-Adresse angezeigt wird.	Checkbox	✗
Fax anzeigen	Legt fest, ob in den Resultaten von Personensuchen eine Spalte für die Faxnummer angezeigt wird.	Checkbox	✗
Fax2 anzeigen	Legt fest, ob in den Resultaten von Personensuchen eine Spalte für die zweite Faxnummer angezeigt wird.	Checkbox	✗
Mobiltelefon anzeigen	Legt fest, ob in den Resultaten von Personensuchen eine Spalte für die Mobiltelefonnummer angezeigt wird.	Checkbox	✗
Personalnummer anzeigen	Legt fest, ob in den Resultaten von Personensuchen eine Spalte für die Personalnummer angezeigt wird.	Checkbox	✗
Personenlöschende Lifecycle-Phasen anzeigen	Gelöschte Personen werden in der Personensuche nicht angezeigt. Daher werden im Suchfilter für Lifecycle-Phasen die Phasen ausgeblendet, welche zur Löschung von Personen suchen, da diese keine Ergebnisse liefern werden. Wird diese Einstellung aktiviert, werden Ihnen diese Phasen im Filter angezeigt. Dies kann nützlich sein, falls Sie die Einstellungen für das Löschen von Personen in einer Phase geändert haben und nun nach Personen suchen möchten, welche sich in diesen Phasen befinden und noch nicht gelöscht sind.	Checkbox	✗
Position anzeigen	Legt fest, ob in den Resultaten von Personensuchen eine Spalte für die Position angezeigt wird.	Checkbox	✗
Ressourcen anzeigen	Legt fest, ob in den Resultaten von Personensuchen eine Spalte für die Account-Ressourcen angezeigt wird.	Checkbox	✗




Stellenbezeichnung anzeigen	Legt fest, ob in den Resultaten von Personensuchen eine Spalte für die Stellenbezeichnung angezeigt wird.	Checkbox	✗
Telefon anzeigen	Legt fest, ob in den Resultaten von Personensuchen eine Spalte für die Telefonnummer angezeigt wird.	Checkbox	✗
Telefon privat anzeigen	Legt fest, ob in den Resultaten von Personensuchen eine Spalte für die private Telefonnummer angezeigt wird.	Checkbox	✗
Telefon2 anzeigen	Legt fest, ob in den Resultaten von Personensuchen eine Spalte für die zweite Telefonnummer angezeigt wird.	Checkbox	✗
User Principal Name anzeigen	Legt fest, ob in den Resultaten von Personensuchen eine Spalte für den User Principal Name angezeigt wird.	Checkbox	✗
>> Requests			
'Alle Abteilungen' anzeigen	Diese Einstellung bestimmt, ob Sie in der Request-Liste die Auswahl "Alle Abteilungen" in den Filtereinstellungen für die Abteilung zur Verfügung haben.	Checkbox	✗
Tage zurück	Mit dieser Einstellung können Sie festlegen, wie viele Tage zurück die Standardeinstellung für "Datum von" in den Filtereinstellungen der Request-Liste beim Betreten der Maske gesetzt ist.	Text	✗
>> Schnellsuche			
Abteilung durchsuchen	Zeigt den Karteireiter "Abteilungen" in der Schnellsuche an.	Checkbox	✗
Active Directory-Tab anzeigen	Zeigt den Karteireiter "Active Directory" in der Schnellsuche an. Diese Einstellung kann individuell pro Person in den persönlichen Schnellsucheinstellungen deaktiviert werden. Ist diese Einstellung nicht aktiv, kann Sie jedoch nicht für einzelne Personen aktiviert werden.	Checkbox	✗
Exchange-Tab anzeigen	Zeigt den Karteireiter "Exchange" in der Schnellsuche an. Diese Einstellung kann individuell pro Person in den persönlichen Schnellsucheinstellungen deaktiviert werden. Ist diese Einstellung nicht aktiv, kann Sie jedoch nicht für einzelne Personen aktiviert werden.	Checkbox	✗

Kostenstelle durchsuchen	Zeigt den Karteireiter "Kostenstellen" in der Schnellsuche an.	Checkbox	
Microsoft 365-Tab anzeigen	Zeigt den Karteireiter "Microsoft 365" in der Schnellsuche an. Diese Einstellung kann individuell pro Person in den persönlichen Schnellsucheinstellungen deaktiviert werden. Ist diese Einstellung nicht aktiv, kann Sie jedoch nicht für einzelne Personen aktiviert werden.	Checkbox	
Niederlassung durchsuchen	Zeigt den Karteireiter "Niederlassungen" in der Schnellsuche an.	Checkbox	
Organisationseinheit durchsuchen	Zeigt den Karteireiter "Organisationseinheit" in der Schnellsuche an. Hinweis: Hierbei handelt es sich um die Stammdatenobjekte der Organisationseinheiten von tenfold, nicht um OUs im Active Directory.	Checkbox	
SharePoint-Tab anzeigen	Zeigt den Karteireiter "SharePoint" in der Schnellsuche an. Diese Einstellung kann individuell pro Person in den persönlichen Schnellsucheinstellungen deaktiviert werden. Ist diese Einstellung nicht aktiv, kann Sie jedoch nicht für einzelne Personen aktiviert werden.	Checkbox	
Telefonnummern durchsuchen	Erlaubt es Personen in der Schnellsuche anhand von Telefonnummern, Faxnummern und Mobiltelefonnummern zu suchen. Diese Einstellung kann individuell pro Person in den persönlichen Schnellsucheinstellungen deaktiviert werden. Ist diese Einstellung nicht aktiv, kann Sie jedoch nicht für einzelne Personen aktiviert werden.	Checkbox	
Verzeichnis-Tab anzeigen	Zeigt den Karteireiter "Verzeichnisse" in der Schnellsuche an. Diese Einstellung kann individuell pro Person in den persönlichen Schnellsucheinstellungen deaktiviert werden. Ist diese Einstellung nicht aktiv, kann Sie jedoch nicht für einzelne Personen aktiviert werden.	Checkbox	
> System			
Ablaufdatum entspricht Ende des Tages	Legt fest, ob das Ablaufdatum einer Person auf das Ende des Tages (23:59:59) oder den Beginn des Tages (00:00:00) gesetzt wird.	Checkbox	
Ablauferinnerung - Tage davor	Legt fest, wie viele Tage bevor das Ablaufdatum einer Person erreicht ist, diese in der Liste der ablaufenden Personen aufscheint.	Text	

Abteilungswechselvorschläge anzeigen	<p>Legt fest, ob auf der Maske für die Abteilungswechsel, die Liste für die Vorschläge der Abteilungswechsel angezeigt wird.</p> <p>Hinweis: Standardmäßig bietet tenfold keine Vorschläge an. Diese müssen durch einen benutzerdefinierten Import-Job erzeugt werden.</p>	Checkbox	
Benutzername automatisch generieren	<p>Legt fest, ob durch Benutzernamenregeln (siehe Regeln für Benutzernamen(see page 585)) ein Benutzername für eine Person erzeugt werden soll, wenn dieser Leer ist. An folgenden Stellen werden die Regeln verwendet um einen Benutzernamen zu generieren:</p> <ul style="list-style-type: none"> • Auf der Maske für Benutzernamensvorschläge bei der Neuanlage einer Person • Beim Betreten der Genehmigungsmaske einer Neuanlage für Personen • Beim Betreten der Maske zur Personenbearbeitung wenn eine neue Person angelegt wird 	Checkbox	





E-Mail-Adresse automatisch generieren	<p>Mit dieser Einstellung wird festgelegt, wie E-Mail-Adressen für neue Personen automatisch generiert werden sollen. Folgende Auswahlmöglichkeiten stehen zur Verfügung:</p> <ul style="list-style-type: none"> • Bei Personenanlage mittels legacy EXEC: Wenn eine neue Person angelegt wird, wird der System EXEC "Person.onEmailSuggestion" aufgerufen. Der zurückgelieferte String wird als E-Mail-Adresse für die neue Person verwendet. • Bei Personenanlage mittels E-Mail-Adressen-Regeln: Wenn eine neue Person angelegt wird, werden die hinterlegten Regeln zur E-Mail-Adresserzeugung (siehe E-Mail-Adressen(see page 600)) verwendet um eine E-Mail-Adresse für die neue Person zu ermitteln. • Bei Ressourcenzuweisung: Die Regeln zur Erzeugung von E-Mail-Adressen werden verwendet um eine Adresse zu erzeugen, wenn dem Benutzer eine Ressource zugeordnet wird, welche ein Postfach anlegt (siehe zum Beispiel Exchange Mailbox Lifecycle(see page 692)). <div style="border: 1px solid green; padding: 10px; margin-top: 10px;"> <p>Keine automatische Erzeugung</p> <p>Wenn Sie nicht wollen, dass tenfold E-Mail-Adressen für Personen erzeugt, können Sie die Einstellung einfach auf "Bei Personenanlage mittels legacy EXEC" belassen. Dieser erzeugt standardmäßig eine leere E-Mail-Adresse.</p> </div>	Auswahl	
Funktionstrennung (Separation of duties) aktiv	<p>Legt fest, ob die Prüfung zur Funktionstrennung bei der Zuweisung von Anwendungsberechtigungen, Ressourcen oder Profilen durchgeführt werden soll. Hinweis: Standardmäßig existieren in tenfold keine Regeln für die Funktionstrennung. Diese werden durch Plugins für bestimmte Fremdsysteme hinzugefügt.</p>	Checkbox	
Funktionstrennungskonflikt (Separation of duties) - Standardquelle	<p>Wenn bei einem Konflikt in der Funktionstrennungsanalyse keine Quelle angegeben wurde, wird stattdessen die hier hinterlegte Quelle verwendet.</p>	Text	






HTTPS-Proxy - Aktiviert	Mit dieser Einstellung legen Sie fest ob tenfold einen Proxy für den Aufbau von HTTP(S)-Verbindungen verwendet.	Checkbox	✗
HTTPS-Proxy - Hostname	Legt den Hostnamen oder die IP-Adresse des Proxys fest, welchen tenfold für den Aufbau von HTTP(S)-Verbindungen verwendet.	Checkbox	✗
HTTPS-Proxy - Port	Legt den Port des Proxys fest, welchen tenfold zur Verbindung über HTTP(S) verwendet.	Checkbox	✗
IDs anzeigen	Ist diese Einstellung aktiv, werden auf diversen Masken in tenfold die Datenbank-IDs der Objekte in Tabellen angezeigt. Hinweis: Nicht zu jeder Tabelle gibt es Objekte hinter welchen Datenbank-IDs liegen.	Checkbox	✗
Intervall Rolle-AD-Abgleich	Legt das zeitliche Intervall in Minuten fest, in welchem tenfold die AD-Gruppenmitgliedschaften mit tenfold-Rollenzuordnungen abgleicht. <div>Manuelle durchführung Sie können den Abgleich jederzeit auf der Maske "Rollen" (Menü > Einstellungen > tenfold-Berechtigungen > Rollen) mittels der Schaltfläche "AD-Gruppen-Zuordnungen aktualisieren" durchführen.</div>	Text	✗
Mehrere Stammdatensätze pro Person - Aktiv	Ist diese Einstellung aktiv, ist es möglich zu jeder Person mehrere Stammdatensätze zu pflegen. Achtung: Aktivieren Sie diese Einstellung nur wenn Sie diese Funktionalität benötigen. Diese wirkt sich auf Speicherauslastung und Performance aus. Auch dann, wenn Personen keine mehreren Stammdatensätze zugeteilt haben.	Checkbox	✗
Mehrere Stammdatensätze pro Person - Bearbeitungsberechtigung überschreiben	Wenn diese Einstellung aktiv ist, können Personen welche die berechtigt sind, den Basisstammdatensatz einer Person zu bearbeiten auch alle weiteren Stammdatensätze bearbeiten, ungeachtet der dort hinterlegten Berechtigungen	Checkbox	✗
Mehrere Stammdatensätze pro Person - Führender Stammdatensatz für Berechtigungsprüfung	Legt fest, ob bei der Verwendung von mehreren Stammdaten pro Person, der Basisstammdatensatz der Datensatz der Person oder der Datensatz der Hauptressource ist.	Checkbox	✗






Mehrere Stammdatensätze pro Person - Löschmodus	<p>Mit dieser Einstellung kann konfiguriert werden, für welche Stammdatensätze einer Person man berechtigt sein muss um die Aktion "Löschen", "Sperren", "Entsperren" und "Verlängern" für diese Person durchführen zu dürfen.</p> <ul style="list-style-type: none"> • Führender Stammdatensatz: Man muss für den Basisstammdatensatz berechtigt sein. • Beliebige Stammdatensätze: Man muss für zumindest einen der Datensätze berechtigt sein. • Alle Stammdatensätze: Man muss für alle Stammdatensätze berechtigt sein. <p>Hinweis: Diese Einstellung hat keine Auswirkung auf die Verwendung der Lifecycle-Phasen. Diese Einstellung ist nur für bestehende Kunden relevant, welche noch nicht auf Lifecycle-Phasen umgestiegen sind.</p>	Auswahl	
Person verlängern - Tage	<p>Legt fest, um wie viele Tage eine Person mit der Aktion "Verlängern" verlängert wird.</p> <p>Hinweis: Diese Einstellung hat keine Auswirkung auf die Verwendung der Lifecycle-Phasen. Diese Einstellung ist nur für bestehende Kunden relevant, welche noch nicht auf Lifecycle-Phasen umgestiegen sind.</p>	Text	
Pfad zu EXEC-Update-Dateien	<p>Legt den Pfad fest, in welchem tenfold nach Updates für die internen EXECs sucht. Diese werden bei Updates kopiert und während des nächsten Starts nach einem Update von tenfold aus diesem Verzeichnis installiert.</p> <div style="border: 1px solid red; padding: 10px; margin-top: 10px;"> <p>Nicht verändern</p> <p>Dieser Eintrag wird bei der Installation von tenfold angelegt und sollte unter normalen Umständen nicht verändert werden.</p> </div>	Text	

Pfad zu tenfold Agent-Update-Dateien	<p>Legt den Pfad fest, in welchem tenfold nach Aktualisierungen für das remote Agent-Update sucht. Diese werden bei Updates von tenfold in dieses Verzeichnis gelegt. Bei remote Updates der Agenten über die Maske der tenfold-Agenten, wird in diesem Verzeichnis nach Updates gesucht.</p> <div> <p>Nicht verändern</p> <p>Dieser Eintrag wird bei der Installation von tenfold angelegt und sollte unter normalen Umständen nicht verändert werden.</p> </div>	Text	✗
Request schließen - Ereignisse bei Abgleichen auslösen	Manche Synchronisierungsprozesse legen Requests in einem sogenannten Silent Mode an, welcher keine Ereignisse beim Abschließen der Requests erzeugt. Dies sorgt dafür, dass nur die Daten in tenfold abgeglichen werden ohne Aktionen auszulösen (z.B. E-Mails versenden). Ist diese Einstellung aktiv, werden trotzdem auch für diesen Silent Mode die normalen Ereignisse beim Schließen der Requests ausgelöst.	Checkbox	✗
Ressourcenzuordnungen beim Löschen einer Person löschen	Wird eine Person gelöscht, wird normalerweise nur ein Request zum Löschen der Person erzeugt. In manchen Szenarien kann es jedoch erforderlich sein, auch Requests zur Löschung der Ressourcen des Benutzers zu erzeugen. Dies können Sie durch aktivieren dieser Einstellung erreichen.	Checkbox	✗
Server-URL für JMS	<p>Legt den Server der Message-Queue fest, welche tenfold zur Kommunikation mit den Agenten verwendet. Ist die Einstellung leer, wird der tenfold-Server verwendet.</p> <p>Achtung: Ändern Sie diese Einstellung nur nach Aufforderung.</p>	Checkbox	✗
System-URL	Hier wird der URL angegeben, auf welchem die tenfold Web-Oberfläche aufrufbar ist. Dieser URL wird von E-Mails verwendet um Links zu generieren, wie z.B. einen Link zur direkten Request-Genehmigung	Text	✗
User Principal Name automatisch generieren	<p>Legt fest, ob der User Principal Name einer Person durch Ressourcen-Zuweisung oder automatisch bei der Personenanlage generiert werden soll.</p> <p>Hinweis: Soll der User Principal Name bei der Personenanlage generiert werden, so muss das Personenfeld "User Principal Name" in den Datensätzen vorhanden sein (siehe Personenarten(see page 81)).</p>	Auswahl	✗

Wartungsmodus	Wird diese Einstellung aktiviert, versetzt sich tenfold in einen Wartungsmodus. In diesem Modus wird auf der Startseite eine Warnung angezeigt, dass sich tenfold im Wartungsmodus befindet und Anmeldungen von Personen welche nicht über die Berechtigung "Use Maintenance Mode" (9120) verfügen, können sich nicht in tenfold anmelden.	Checkbox	✗
Zukünftige Personenänderung - Zusammenführungsmodus	Während Sie auf der Maske zur Bearbeitung von Personen eine zukünftige Änderung anlegen, werden Ihnen die voraussichtlichen Daten zum Durchführungszeitpunkt der Änderung angezeigt. Mit dieser Einstellung können Sie festlegen ob bei der Anzeige alle Requests für zukünftige Änderungen bis zu diesem Zeitpunkt berücksichtigt werden soll oder nur jene, welche zum aktuellen Zeitpunkt bereits genehmigt sind.	Auswahl	✗
> User Interface Komponenten			
Anwendungsberechtigungen-Baum - Schwellenwert	Gibt die Anzahl von Anwendungsberechtigungen an, ab welcher Berechtigungen in einem Dialog angezeigt werden, statt direkt in den Baum geladen zu werden.	Text	✗
Auto-Vervollständigung - Verzögerung	Mit dieser Einstellung kann die Anzahl in Millisekunden festgelegt werden, welche nach der Eingabe in Feldern mit Auto-Vervollständigung gewartet wird, bis die Vorschläge geladen werden.	Text	✗
Benutzernamensvorschlag - Abteilung und Niederlassung anzeigen	Legt fest, ob Abteilung und Niederlassung auf der Maske für Benutzernamensvorschläge angezeigt werden.	Checkbox	✗
Berechtigungstypgruppen - Größe	Legt fest, wie viele Berechtigungstypen zu einer Gruppe zusammengefasst werden, sobald der Schwellenwert zur Gruppenbildung erreicht wird.	Text	✗
Berechtigungstypgruppen - Schwellenwert	Legt fest, ab wie vielen Berechtigungstypen, die Baumansicht der Berechtigungen zu alphabetischen Gruppen zusammengefasst wird.	Text	✗
HTML-Titel	Gibt an, welcher Website-Titel im Browser beim Benutzern der tenfold-Oberfläche angezeigt wird.	Text	✗

Logo	<p>Mit diesem Parameter kann ein URL angegeben werden, welcher als Quelle für das Logo in der tenfold-Oberfläche verwendet wird. Dieser Pfad kann absolut angegeben werden oder relativ zum Basis-URL der tenfold-Anwendung (https://<server>:<port>/tenfold).</p> <p>Achtung: Verwenden Sie für den URL des Logos das HTTPS-Protokoll. Andernfalls wird Ihnen Ihr Browser eine Sicherheitswarnung beim Browsen durch die tenfold-Anwendung anzeigen.</p>	Text	
Logo-Style	<p>Gibt einen benutzerdefinierten CSS-Stil an, welcher für die Anzeige des Logos verwendet wird. Verwenden Sie dieses, um die Anzeige Ihres Logos zu verbessern, wenn dieses sonst nicht gut in die tenfold-Oberfläche passt. Sollten Sie das Standard-Logo von tenfold verwenden, können Sie diese Einstellung einfach leer lassen.</p>	Text	
Person löschen - Option 'Sicherung erforderlich' anzeigen	<p>Mit dieser Einstellung kann aktiviert werden, dass beim Löschen von Personen ein Dialog angezeigt wird, welcher die Option zur Sicherung der Personendaten anbietet. Ohne benutzerdefinierte Anpassungen, haben die Auswahlmöglichkeiten dieses Dialoges jedoch keine Auswirkung.</p> <p>Achtung: Diese Einstellung funktioniert nur mit der Legacy-Aktion "Person Löschen", welche in älteren Installationen vor der Einführung der Lifecycle-Phasen vorhanden war. Diese Einstellung hat keinerlei Auswirkung mehr, sobald Ihre Installation mit Lifecycle-Phasen arbeitet. Diese Einstellung ist nur für Legacy-Installationen relevant.</p>	Checkbox	
tenfold-Theme	<p>Mit dieser Einstellung können Sie ein Farbschema für die Titel- und Menüleiste von tenfold festlegen. Sie können dies Benutzen um Ihr Logo besser in tenfold einzupassen.</p> <div style="border: 1px solid green; padding: 10px; margin-top: 10px;"> <p>Testsystem</p> <p>Sollten Sie in Ihrer Umgebung Test- und Produktivsysteme von tenfold eingerichtet haben, verwenden Sie unterschiedliche Themen, um optisch besser zwischen den Systemen unterscheiden zu können.</p> </div>	Text	

Änderungsinformationen anzeigen	<p>Definiert, ob auf verschiedenen Stammdatenmasken die Möglichkeit angeboten wird, Informationen zu Änderungen der Stammdaten anzuzeigen. Diese Informationen enthalten:</p> <ul style="list-style-type: none"> • Datum der Anlage • Ersteller des Datensatzes • Datum der letzten Änderung • Person welche die letzte Änderung durchgeführt hat <p>Hinweis: Nicht für alle Stammdatenobjekte wird diese Information geführt.</p>	Checkbox	
>> Abteilungen			
Abteilungsauswahl - Hierarchie anzeigen	Mit dieser Einstellung kann festgelegt werden, ob in Auswahlfeldern für Abteilungen, die Hierarchiedetails zu den Abteilungen angezeigt werden (die übergeordneten Abteilungen).	Checkbox	
Kurznamen anzeigen	Mit dieser Einstellung kann festgelegt werden, ob in Auswahlfeldern für Abteilungen, der Kurzname der Abteilungen angezeigt werden soll.	Checkbox	
>> Active Directory-Objekte			
Mindestzeichen für Auto-Vervollständigung	Gibt an, wie viele Zeichen in Suchfeldern für Active Directory-Objekte eingegeben werden müssen, bevor Vorschläge zur Autovervollständigung gemacht werden.	Text	
>> Kostenstellen			
Kostenstellenauswahl - Anzeigereihenfolge	<p>Legt fest ob die Auswahlfelder für Kostenstellen zuerst den Code oder zuerst den Namen führen sollen. Also ob eine Kostenstelle "IT" mit dem Code "00001" als "IT - 00001" oder als "00001 - IT" geführt werden soll.</p> <p>Hinweis: Dies hat auch auf die Sortierung der Auswahllisten eine Auswirkung.</p>	Auswahl	
>> Niederlassungen			

Niederlassung erstellen - Suche ähnlicher Niederlassungen mit Wildcards	Wenn Sie beim Anlegen einer Person eine Niederlassung erstellen, wird vor dem Speichern nach Niederlassungen gesucht, welche den angegebenen Namen der neuen Niederlassung enthalten, um zu vermeiden, dass Niederlassungen doppelt angelegt werden. Wird diese Einstellung aktiviert, werden mehrere Wildcards im Niederlassungsnamen platziert, dadurch werden potentiell mehrere ähnliche Niederlassungen gefunden.	Checkbox	
Niederlassung erstellen - Telefon-Feld aktualisieren	Wird diese Einstellung aktiviert, wird das Feld "Telefon" der Person auf das Feld "Telefon" einer neu angelegten Niederlassung gesetzt, wenn das Personenfeld leer ist und die Niederlassung während des Bearbeitens einer Person erstellt wurde. Hinweis: Dies ist eine Legacy-Einstellung, verwenden Sie besser einen generierten Wert (siehe Generierte Werte (see page 603)) um das Feld "Telefon" abhängig von der Niederlassung zu befüllen.	Checkbox	
Niederlassungsauswahl - Unternehmen anzeigen	In tenfold ist vorgesehen, dass jede Niederlassung zu genau einem Unternehmen gehören kann. Wenn an einer Niederlassung mehrere Unternehmen vorhanden sind, muss in tenfold für jedes Unternehmen am selben Standort eine eigene Niederlassung angelegt werden. Um diese Niederlassungen beim bearbeiten einer Person besser unterscheiden zu können (ohne diesen einen eigenen Namen geben zu müssen), kann durch Aktivieren dieser Einstellung das Unternehmen bei der Niederlassungsauswahl angezeigt werden.	Checkbox	
Niederlassungsdialog Anzeigemodus verfügbar	Wird diese Einstellung aktiviert, wird im Anzeigemodus der Personenmaske, die ausgewählte Niederlassung als Link dargestellt, welcher einen Dialog mit den Daten der Niederlassung anzeigt.	Checkbox	
Niederlassungsdialog Bearbeitungsmodus verfügbar	Wird diese Einstellung aktiviert, erscheint in der Maske zur Personenbearbeitung eine Schaltfläche bei der Niederlassungsauswahl, welcher einen Dialog mit den Details zu ausgewählten Niederlassung einblendet.	Checkbox	
>> Warnungen			

Person bearbeiten: Warnung bei ungespeicherten Requests anzeigen	Ist diese Einstellung aktiv, wird Ihnen beim Verlassen der Maske zur Personenbearbeitung eine Warnung angezeigt, wenn sich ungespeicherte Änderungen auf der Maske befinden.	Checkbox	✗
Self-Service: Warnung bei ungespeicherten Requests anzeigen	Ist diese Einstellung aktiv, wird Ihnen beim Verlassen des Self-Service-Bereichs eine Warnung angezeigt, wenn sich ungespeicherte Requests in Ihrer Liste befinden.	Checkbox	✗
Webserver			
HTTP-Session-Timeout	Legt den Zeitraum fest, nach welchem eine Benutzersitzung ohne Interaktion verworfen wird. Dieser Zeitraum wird in Minuten angegeben.	Text	✗
JSF-Conversation-Timeout	Legt das JSF-Conversation-Timeout fest. Dieser Wert wird in Minuten angegeben.	Text	✗
JSF-Conversation-Timeout für gleichzeitigen Zugriff	Legt das JSF-Conversation-Timeout für gleichzeitigen Zugriff fest. Dieser Wert wird in Minuten angegeben.	Text	✗
Template für HTTP-Schnittstellen	Definiert die Standardvorlage für HTTP-Interface-Antworten.	Checkbox	✗
>> Cookies			
HttpOnly-Flag	Aktiviert das HttpOnly-Flag für den Session-Cookie von tenfold. Hierbei handelt es sich um eine Sicherheitseinstellung, welche aktiviert werden sollte. Diese bewirkt, dass der Session-Cookie nicht von Skripten auf der Webseite verändert werden kann und verhindert damit XSS-Attacken.	Checkbox	✓
Secure-Flag	Diese Einstellung aktiviert das Secure-Flag im Session Cookie von tenfold. Mit dieser Einstellung ist es nach Erzeugung des Cookies nur mehr möglich den Cookie über HTTPS-Verbindungen zu ändern. Achtung: Diese Einstellung darf erst aktiviert werden, nachdem ein gültiges HTTPS-Zertifikat hinterlegt wurde und die automatische Weiterleitung auf HTTPS konfiguriert wurde.	Checkbox	✓
>> HTTP-Header			

Cache-Control	Legt den Wert des "Cache-Control" HTTP-Headers fest, welcher von tenfold an Browser gesendet wird. Eine Beschreibung des Headers finden sie unter: https://developer.mozilla.org/de/docs/Web/HTTP/Headers/Cache-Control . Möchten Sie diesen Header deaktivieren (wird nicht empfohlen!), so ändern Sie den Wert auf "DISABLED"	Text	✓
Content-Security-Policy	Legt den Wert des "Content-Security-Policy" HTTP-Headers fest, welcher von tenfold an Browser gesendet wird. Eine Beschreibung des Headers finden Sie unter: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP . Möchten Sie den Header deaktivieren (wird nicht empfohlen!), ändern Sie den Wert auf "DISABLED".	Text	✓
Expires	Legt den Wert des "Expires" HTTP-Headers fest, welcher von tenfold an Browser gesendet wird. Eine Beschreibung des Headers finden Sie unter: https://developer.mozilla.org/de/docs/Web/HTTP/Headers/Expires . Möchten Sie den Header deaktivieren (wird nicht empfohlen!), ändern Sie den Wert auf "DISABLED".	Text	✓
Pragma	Legt den Wert des "Pragma" HTTP-Headers fest, welcher von tenfold an Browser gesendet wird. Eine Beschreibung des Headers finden Sie unter: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Pragma . Möchten Sie den Header deaktivieren (wird nicht empfohlen!), ändern Sie den Wert auf "DISABLED".	Text	✓
Referrer-Policy	Legt den Wert des "Referrer-Policy" HTTP-Headers fest, welcher von tenfold an Browser gesendet wird. Eine Beschreibung des Headers finden Sie unter: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy . Möchten Sie den Header deaktivieren (wird nicht empfohlen!), ändern Sie den Wert auf "DISABLED".	Text	✓
Strict-Transport-Security	Legt den Wert des "Strict-Transport-Security" HTTP-Headers fest, welcher von tenfold an Browser gesendet wird. Eine Beschreibung des Headers finden Sie unter: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security . Möchten Sie den Header deaktivieren (wird nicht empfohlen!), ändern Sie den Wert auf "DISABLED".	Text	✓

X-Content-Type-Options	Legt den Wert des "X-Content-Type-Options" HTTP-Headers fest, welcher von tenfold an Browser gesendet wird. Eine Beschreibung des Headers finden Sie unter: https://developer.mozilla.org/de/docs/Web/HTTP/Headers/X-Content-Type-Options . Möchten Sie den Header deaktivieren (wird nicht empfohlen!), ändern Sie den Wert auf "DISABLED".	Text	✓
X-Frame-Options	Legt den Wert des "X-Frame-Options" HTTP-Headers fest, welcher von tenfold an Browser gesendet wird. Eine Beschreibung des Headers finden Sie unter: https://developer.mozilla.org/de/docs/Web/HTTP/Headers/X-Frame-Options . Möchten Sie den Header deaktivieren (wird nicht empfohlen!), ändern Sie den Wert auf "DISABLED".	Text	✓
X-XSS-Protection	Legt den Wert des "X-XSS-Protection" HTTP-Headers fest, welcher von tenfold an Browser gesendet wird. Eine Beschreibung des Headers finden Sie unter: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection . Möchten Sie den Header deaktivieren (wird nicht empfohlen!), ändern Sie den Wert auf "DISABLED".	Text	✓

12.8 Berichtvorlagen

Die Berichtvorlagen dienen dazu, Berichte, die aus tenfold generiert werden, mit bestimmte Voreinstellungen zu belegen, damit diese nicht bei jeder Berichtsausführung individuell konfiguriert werden müssen. Einerseits kann dies aufwändig sein, andererseits können über Vorlagen Berichte für Anwender aus non-IT-Bereichen erstellt werden. Diese Anwender verfügen üblicherweise nicht über die notwendigen Kenntnisse, um die einzelnen Einstellungen der Berichte zu verstehen. Sie müssen aber trotzdem die Möglichkeit haben, Daten in Form von Berichten aus dem System exportieren zu können.

Benötigte Berechtigung

Um diese Funktion nutzen zu können, ist die Systemberechtigung "Manage Report Templates" (3200) erforderlich.

Die anschließenden Optionen sind für alle Berichte gleichermaßen gültig. Bei Optionen, die nur für bestimmte Berichte relevant sind, wird auf diesen Umstand explizit hingewiesen.

Es können neue Vorlagen über den Button "Neu" angelegt werden. Über das Kontextmenü können bestehende Vorlagen bearbeitet, kopiert und gelöscht werden.

Für jede Vorlage können folgende Daten festgelegt werden:

- Name: Bezeichnung auf der tenfold-Oberfläche
- Icon: Das ausgewählte Icon erscheint auf der entsprechenden Kachel, wenn der Benutzer zwischen den für ihn verfügbaren Vorlagen auswählt
- Beschreibung: Es kann eine Beschreibung hinterlegt werden. Diese ist ebenfalls in der Kachel sichtbar und soll für den Benutzer die Einstellungen aus der Vorlage auf verständliche Weise erklären.
- Sichtbar für Dateneigentümer: Wenn diese Option aktiviert ist, kann diese Vorlage im Dateneigentümer-Modus ausgewählt werden. Ist sie nicht aktiviert, so steht sie nur im Administrator-Modus zur Verfügung.

Spezifische Optionen

Die Optionen, welche unterhalb angezeigt werden, sind spezifisch für den jeweiligen Bericht. Aktuell werden Vorlagen nur für den Fileserver-Bericht unterstützt. Die Bedeutung der Einstellungen sind unter [Verwaltung der Fileserver-Berechtigungen](#) (see page 269) ersichtlich.

12.9 Sessionverwaltung

12.9.1 Aktuelle Sessions

Benötigte Berechtigung

Um diese Funktion nutzen zu können, muss der Benutzer über die Systemberechtigung "View Current Sessions" (8081) verfügen.

Die Anwendung bietet eine Möglichkeit, um anzuzeigen, welche Benutzer aktuell angemeldet sind. Hierzu navigieren Sie im Menü zu "Einstellungen > Sessionverwaltung > Aktuelle Sessions".

The screenshot shows the 'tenfold' web application interface. The top navigation bar includes links for 'Personen', 'Ressourcen', 'Berechtigungen', 'Requests', 'Organisation', 'Workflows', 'Provisioning', and 'Einstellungen'. The main content area is titled 'Sessionverwaltung' and 'Aktuelle Sessions'. It contains two tables:

Nachahmen (0)			
Nachname	Vorname	Benutzername	Personalnummer
Keine Einträge vorhanden			

Aktive HttpSessions (2)								
Nachname	Vorname	Benutzername	Personalnummer	Sitzung angelegt	Letzter Zugriff	Leerlauf seit	Ablaufdatum	ID
Sammelmayr	Helmut	sysism		21.08.2017 13:47:16	21.08.2017 16:50:56	01:07:52	22.08.2017 16:50:56	FRVZZBtzrUq9e0l8
Sammelmayr	Helmut	sysism		21.08.2017 16:51:07	21.08.2017 17:58:48	00:00:00	22.08.2017 17:58:48	JStoZSaR7BxtTjIC1

Im Bereich "Aktive HTTP Session" werden alle Benutzer aufgelistet, welche aktuell über das Web-Frontend verbunden sind. Folgende Detailinformationen werden in der Tabelle angezeigt:

- Nachname / Vorname / Benutzername / Personalnummer des betroffenen Benutzers
- Sitzung angelegt: Datum und Uhrzeit, wann der Benutzer sich angemeldet hat
- Letzter Zugriff: Datum und Uhrzeit des Zeitpunkts, an dem die letzte Interaktion stattgefunden hat (z.B. Klick auf einen Button oder einen Menüeintrag)
- Ablaufdatum: Zu diesem Zeitpunkt wird die Session des Benutzers ablaufen, wenn keine weitere Interaktion stattfindet. Der Benutzer muss sich anschließend neu anmelden.
- ID: Die interne Session ID. Die Information ist ausschließlich bei Programmfehlern von Interesse

Im Bereich "Nachahmen" werden alle Session aufgezeigt, bei denen ein Benutzer die Rolle eines anderen Benutzers übernommen hat. Siehe dazu den Punkt "Session ändern".

Achtung

Es werden an diesem Punkt keine Verbindungen von oder zu tenfold Agents oder Verbindungen über HTTP Interfaces aufgelistet.

12.9.2 Session ändern

Benötigte Berechtigung

Um diese Funktion nutzen zu können, muss der Benutzer über die Systemberechtigung "View Current Sessions" (8081) verfügen.

Mit der Funktion "Session ändern" können Sie in die Rolle eines anderen Benutzers schlüpfen und dessen Berechtigungen übernehmen. Um diese Funktion zu nutzen gehen Sie wie folgt vor:

- Navigieren Sie im Menü zu "Einstellungen > Sessionverwaltung > Session ändern"
- Wählen Sie im Eingabefeld die Person aus, deren Berechtigungen Sie übernehmen wollen
- Drücken Sie auf den Button "Nachahmen"

Die Anwendung startet anschließend eine Session mit dem ausgewählten Benutzer. Sie sehen alle Punkte in der Anwendung genau so, wie der Benutzer sie sehen würde, wenn er sich anmeldet (mit der Ausnahme, dass die Berechtigung "View Current Sessions" (8081) in der Session verfügbar ist, unabhängig davon, ob der ausgewählte Benutzer tatsächlich über die Berechtigung verfügt. Sie ist erforderlich, damit die Session wieder auf den ursprünglichen Benutzer zurückgeändert werden kann).

Achtung

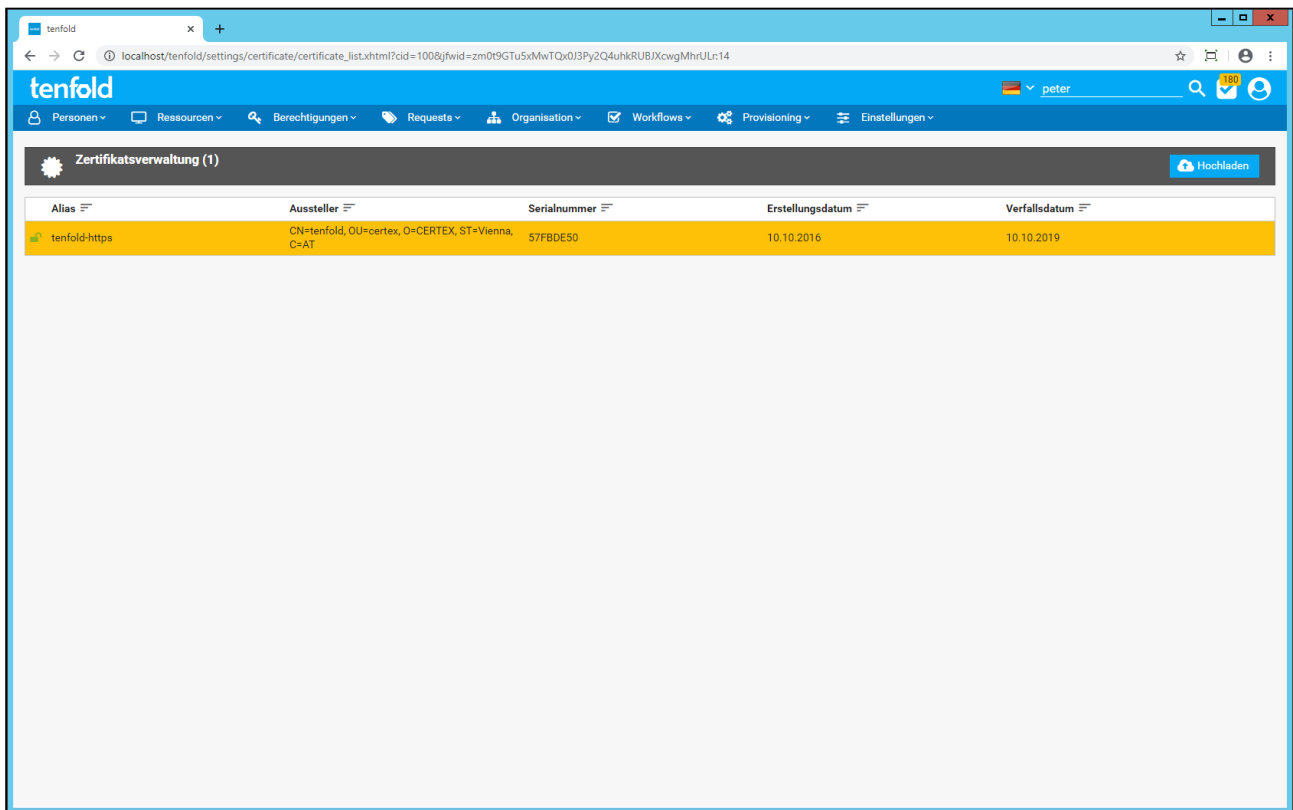
Diese Funktion dient primär dem Testen von konfigurierten Berechtigungen innerhalb von tenfold. Sie darf auf keinen Fall dazu genutzt werden, um Berechtigungen des betroffenen Benutzers missbräuchlich zu verwenden.

12.10 Zertifikatsverwaltung

In der Zertifikatsverwaltung kann das HTTPS-Zertifikat für den tenfold-Webserver ausgetauscht werden. Im Installationszustand ist bereits ein selbstsigniertes Zertifikat eingespielt, welches für den produktiven Betrieb jedoch unbedingt ausgetauscht werden sollte. Die Maske kann über das Menü > Einstellungen > Zertifikate erreicht werden.

Benötigte Berechtigung

Für die Verwaltung der Zertifikate ist die Systemberechtigung "Manage Certificates" (8092) erforderlich



Um das bestehende Zertifikat auszutauschen, muss man auf den Button "Hochladen" klicken und anschließend das Zertifikat mit dem alias "tenfold-https" ersetzen. Aktuell wird das Hinzufügen von Zertifikaten für andere Dienste, wie beispielsweise LDAPS, über diese Maske nicht unterstützt.

Hinweis

Nachdem das Zertifikat erfolgreich installiert wurde, muss der Dienst "tenfold Server" neu gestartet werden.

12.11 Softwarelizenz

12.11.1 Allgemeines

tenfold funktioniert nur, wenn eine gültige Softwarelizenz vorhanden ist. Lizenzen werden in verschlüsselten Textdateien ausgeliefert und müssen in tenfold eingespielt werden, damit sie erkannt und verwendet werden können.

Eine Lizenzdatei hat folgende wichtige Merkmale, die im Dateiinhalte verschlüsselt sind:

- Lizenznehmer: Gibt an, wer Eigentümer der Lizenz ist.
- Anzahl Benutzer: Definiert, wie viele aktive, physische Benutzerkonten über diese Lizenz verwaltet werden dürfen.
- Features (Edition): Legt fest, welche Funktionen von tenfold mit dieser Lizenz genutzt werden dürfen. Nicht lizenzierte Funktionen werden systemseitig gesperrt.
- Ablaufdatum: Gibt an, bis wann die Lizenz gültig ist. Unbefristete Lizenzen sind bis zum 31.12.2999 gültig.

tenfold prüft lediglich das Ablaufdatum der Lizenz. Ist das Ablaufdatum überschritten, so kann tenfold nicht mehr verwendet werden. Die Anzahl der lizenzierten Benutzer wird angezeigt, allerdings wird die Funktionalität nicht eingeschränkt, wenn die Anzahl der tatsächlich verwalteten Benutzer die Anzahl der lizenzierten Benutzer überschreitet.

Benachrichtigung

Während der Funktionsumfang von tenfold nicht durch eine Unterlizenzierung eingeschränkt wird, erhalten Sie dennoch regelmäßig Warnungen, sollte die Anzahl der lizenzierten Objekte überschritten werden.

Achtung - Lizenzieren Sie korrekt!

Die ordnungsgemäße Lizenzierung ist unabhängig von der technischen Überprüfung zwingend erforderlich. Wird eine Lizenz in jeglicher Weise unrechtmäßig genutzt, so stellt dies eine Vertragsverletzung der tenfold EULA dar. Dies kann etwaige Schadenersatzansprüche zur Folge haben.

12.11.2 Installation einer neuen Lizenz

Um eine neue Lizenz im System zu installieren, muss diese lediglich an den dafür vorgesehenen Ort kopiert werden. Die Default-Einstellung für die Lizenzdatei ist C:\tenfold\license\tenfold.lic. tenfold versucht beim Server-Start zuerst die eingestellte Datei zu laden. Existiert diese Datei nicht, oder ist sie nicht mehr gültig, dann sucht tenfold alphabetisch nach weiteren Dateien im gleichen Verzeichnis. Es wird die erste gültige Lizenzdatei verwendet, die gefunden wird. Anschließend wird nicht nach weiteren Dateien gesucht.

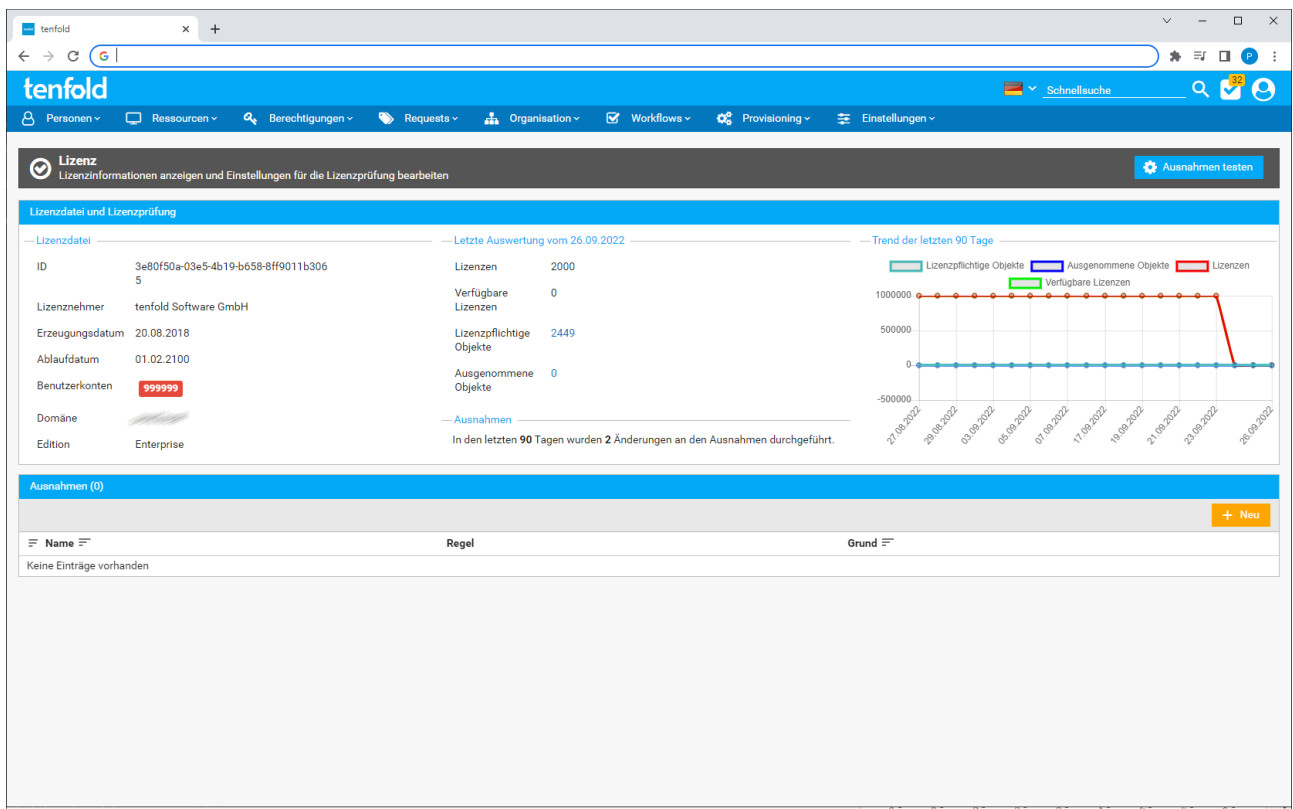
Es ist somit ausreichend, eine neue Lizenzdatei einfach in den Ordner C:\tenfold\license\ zu kopieren.

12.11.3 Lizenzeinstellungen

Um die Einstellungen Ihrer Lizenz zu verwalten, navigieren Sie im Menü auf die Maske *Einstellungen > System > Lizenz*.

Benötigte Berechtigung

Für die Verwaltung ist die Berechtigung "Manage License" (9210) erforderlich.



Im Bereich "Lizenzdatei" rechts finden Sie eine Reihe von Informationen zu Ihrer Lizenz.

Feld	Beschreibung
Lizenznehmer	Hier finden Sie den Namen des Unternehmens, auf das die Lizenz ausgestellt wurde.
Erzeugungsdatum	Zeigt an, an welchem Datum die Lizenz erzeugt wurde.
Ablaufdatum	Gibt an, bis zu welchem Datum die Lizenz gültig ist. Hinweis: Nicht alle Lizenzen werden mit einem Ablaufdatum ausgestellt.
Benutzerkonten	Zeigt die Anzahl der Benutzerkonten an, für die tenfold lizenziert wurde.
Domäne	Zeigt an, für welche Domäne tenfold lizenziert wurde. Hinweis: Hierbei handelt es sich um den Namen der Domäne, in welcher der tenfold-Server betrieben werden darf, nicht um die Domäne oder Domänen, welche von tenfold verwaltet werden.
Edition	Hier wird die lizenzierte Edition von tenfold angegeben. Diese spiegelt den Leistungsumfang wieder, welchen tenfold in Ihrer Umgebung enthält.

Editionsupgrade

Eine Erhöhung der tenfold-Edition ist jederzeit durch Erwerb und Installation einer neuen Lizenz möglich. Eine Neuinstallation von tenfold ist hierfür **nicht** erforderlich.

Darüber hinaus erhalten Sie im Bereich "Auswertung" Informationen über die Auslastung Ihrer lizenzierten Benutzerkonten. Hierbei wird Ihnen angezeigt, wieviele lizenzierungspflichtige Objekte tatsächlich vorhanden sind und wieviele Objekte Ihnen damit noch übrig bleiben. Ebenso wird Ihnen eine Trendgrafik angezeigt, welche die Veränderung der lizenzierungspflichtigen Objekte in den letzten 90 Tagen anzeigt. Dieser Trend kann Ihnen dabei helfen frühzeitig zu erkennen, ob die Beschaffung neuer Lizenzen notwendig ist, um eine Unterlizenzierung zu vermeiden.

Lizenzierungspflichtige Objekte werden dabei wie folgt gezählt:

- Alle Personenobjekte in tenfold.
- Alle Active Directory-Objekte in tenfold, welche keiner Person zugeordnet wurden.
- Alle Microsoft 365-Objekte in tenfold, welche keiner Person zugeordnet wurden.

Personen- und Domänenobjekte

Da für die Lizenzierung jede Person nur einmal gezählt wird, werden Objekte aus dem Active Directory und Microsoft 365, die einer Person zugeordnet wurden, nicht hinzugezählt.

Ausgeschlossene Bereiche

Sie können in den Einstellungen zur Active Directory-Domäne OUs aus dem Scan ausschließen oder den Bereich nur auf bestimmte OUs einschränken. Sollten im Scanbereich jedoch Gruppen mit Mitgliedern gefunden werden, welche sich außerhalb des Scanbereichs befinden, scannt tenfold diese Objekte trotzdem, um diese korrekt darstellen zu können. Diese Objekte werden für die Lizenz **nicht** mitgezählt, können mittels tenfold jedoch auch nicht verwaltet werden. Diese Objekte werden nur angezeigt.

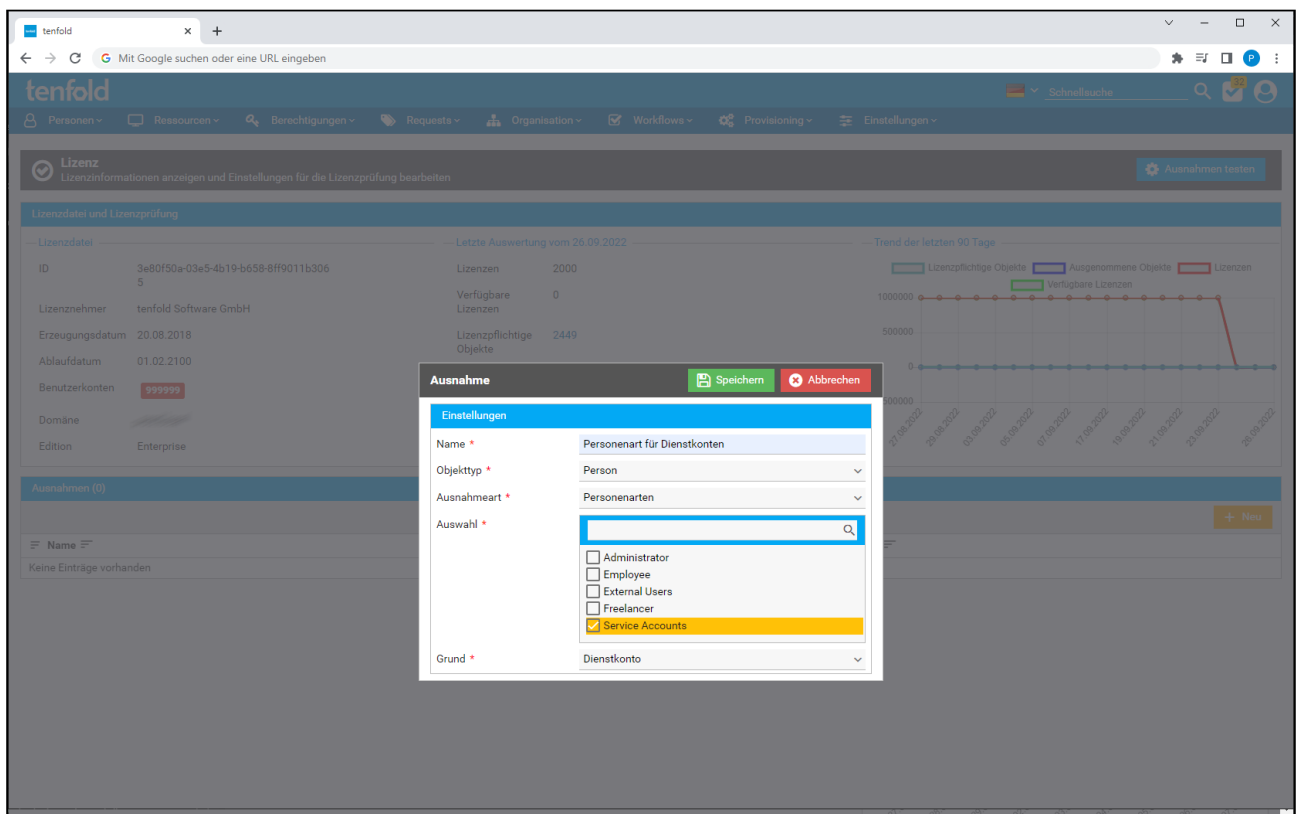
Ausnahmen festlegen

Grundsätzlich sind nur real existierende Personen lizenzierungspflichtig. Administratorkonten, Dienstkonten und dergleichen müssen nicht lizenziert werden, jedoch ist die Verwaltung solcher Konten durch tenfold möglich und gestattet. Da es nicht möglich ist, automatisch zu erkennen, ob ein eingelestes Objekt lizenzierungspflichtig ist oder nicht, können Regeln festgelegt werden, um zu bestimmen, welche Objekte von der Lizenzierungspflicht ausgenommen werden.

Änderungsprotokoll

Auf der Maske wird angezeigt, wie viele Änderungen des Regelwerkes in den letzten 90 Tagen getätigt wurden. Zusätzlich dazu werden von tenfold intern sämtliche Änderungen im Detail protokolliert. Diese können bei anfallenden Lizenzprüfungen kontrolliert werden.

Im Bereich "Ausnahmen" auf der Maske werden alle bisher definierten Ausnahmen tabellarisch dargestellt. Mittels der Schaltfläche "Neu" können Sie eine neue Ausnahme hinzufügen.



Im Dialog können Sie folgende Einstellung für die neue Ausnahme treffen:

Einstellung	Beschreibung
Name	Legt den Namen der Regel fest.
Objekttyp	<p>Legt die Art von Objekten fest, auf welche sich die Regel bezieht. Zur Auswahl stehen:</p> <ul style="list-style-type: none"> • Person • Active Directory-Objekt • Microsoft 365-Objekt <p>Achtung: Active Directory- und Microsoft 365-Objekte, welche mit Personen verknüpft sind, werden von der Zählung grundsätzlich ausgenommen. Die Ausnahmeregeln haben auf diese Objekte keine Auswirkung.</p>
Ausnahmeart	Legt fest, auf welche Eigenschaft der ausgewählten Objekte die Regel Bezug nimmt.
Ausnahmearten für Objekttyp "Person"	
Benutzername	Die Personen werden auf das Personenfeld "USERID" (Benutzername) geprüft.

User Principal Name	Die Personen werden auf das Personenfeld "USER_PRINCIPAL_NAME" (User Principal Name) geprüft. Achtung: Damit diese Überprüfung korrekte Ergebnisse liefern kann, muss das Feld User Principal Name in den Feldern der jeweiligen Personen hinterlegt und entsprechend gemappt werden.
Person	Legt eine einzelne Person fest, welche von der Zählung ausgenommen wird.
Personenarten	Legt eine oder mehrere Personenarten fest, deren Personen von der Zählung ausgenommen werden.
Lifecycle-Phasen	Legt eine oder mehrere Lifecycle-Phasen fest, von denen alle Personen ausgenommen werden, die sich in diesen befinden.
Ressourcen	Bestimmt eine oder mehrere Ressourcen. Alle Personen, welche eine Zuordnung zu dieser Ressource besitzen, werden von der Zählung ausgenommen.
Ausnahmearten für Objekttyp "Active Directory-Objekt"	
Benutzername	Prüft auf das Attribut "sAMAccountName", ob das Objekt von der Zählung ausgeschlossen wird.
User Principal Name	Prüft auf das Attribut "userPrincipalName", ob das Objekt von der Zählung ausgeschlossen wird.
Kategorien	Alle Active Directory-Objekte, welche den ausgewählten Kategorien zugeordnet sind, werden von der Zählung ausgeschlossen.
Organisationseinheit	Prüft die Active Directory OU, in welcher sich das Objekt befindet, um zu entscheiden, ob das Objekt von der Zählung ausgeschlossen wird. Alle Objekte innerhalb dieser OU oder darunter werden ausgeschlossen.
Ausnahmearten für Objekttyp "Microsoft 365-Objekt"	
User Principal Name	Prüft auf das Attribut "userPrincipalName" im Azure Active Directory.
Überprüfungsarten für Textfelder/-Attribute	
Beginnt mit	Das Feld oder Attribut wird darauf geprüft, ob es mit dem eingegebenen Wert beginnt. (Beispiel: Alle Active Directory-Konten, deren Benutzername mit "adm-" beginnen.)
Endet mit	Das Feld oder Attribut wird darauf geprüft, ob es mit dem eingegebenen Wert endet. (Beispiel: Alle Active Directory-Konten, deren Benutzername mit ".svc" enden.)

Enthält	Das Feld oder Attribut wird darauf geprüft, ob es den eingegebenen Wert enthält (Beginn, Ende oder in der Mitte).
Ist gleich	Es wird nur darauf geprüft, ob das Feld oder Attribut exakt dem eingegebenen Wert entspricht.
Regulärer Ausdruck	Es wird geprüft, ob das Feld oder Attribut eine Übereinstimmung für den eingegebenen regulären Ausdruck liefert.
Grund für die Regel	
Grund	Es muss ein Grund ausgewählt werden, warum die Objekte, welche auf diese Regel zutreffen, von der Zählung ausgenommen werden sollen. Folgende Optionen stehen zur Auswahl: <ul style="list-style-type: none"> • Administratorkonto • Dienstkonto • Testbenutzer • Sonstiges
Text	Wurde im Feld "Grund" die Auswahl "Sonstiges" getroffen, muss in dieser Einstellung ein Freitext eingetragen werden, der den Grund für die Ausnahme beschreibt.

Mit der Schaltfläche "Speichern" können Sie die Anlage der neuen Regel abschließen.

Im Aktionsmenü der jeweiligen Regel können Sie mit der Aktion "Bearbeiten" den Dialog erneut öffnen, um die Einstellungen der Regel zu bearbeiten und die Änderungen mit der Schaltfläche "Speichern" festzuschreiben. Mit der Aktion "Löschen" können Sie bestehende Regeln wieder entfernen.

Änderungen sofort wirksam

Im Gegensatz zu vielen anderen Masken werden Änderungen, die im Dialog vorgenommen wurden sowie Zeilen der Tabelle, die gelöscht wurden, sofort gespeichert.

Auswertung

Einmal täglich findet eine Auswertung der Lizenzen statt. Hierbei wird anhand der gezählten, ausgenommenen und in der Lizenz verfügbaren Objekte ermittelt, wie viele Lizenzen Ihnen noch zur Verfügung stehen.

Im Abschnitt "Letzte Auswertung vom <Datum>" erhalten Sie dabei eine Übersicht über die Zählung.

Feld	Beschreibung
Lizenz	Gibt an, wie viele Objekte in der Lizenz enthalten sind. Dies entspricht dem Wert "Benutzerkonten" im Abschnitt "Lizenzdatei".
Verfügbare Lizenzen	Zeigt an, wie viele Objekte Sie in Ihrer Lizenz noch zur Verfügung haben.
Gesamtzahl der Objekte	Gibt an, wie viele Objekte gesamt gezählt wurden, ungeachtet der Ausnahmen.
Ausgenommene Objekte	Gibt an, wie viele Objekte aus der Zählung anhand der eingestellten Ausnahmen von der Zählung ausgenommen wurden.

Feld	Beschreibung
Lizenzpflichtige Objekte	Zeigt Ihnen an, wie viele Lizenzpflichtige Objekte gezählt wurden, nachdem die Ausnahmen von der Gesamtzahl abgezogen wurden.

12.11.4 Mögliche Probleme

Folgende Probleme können bei der Lizenzprüfung auftreten, welche die ordnungsgemäße Nutzung von tenfold verhindern.

Keine Lizenzdatei gefunden

Wird keine gültige Lizenzdatei gefunden, so enthält die Logdatei (server.log) folgende Fehlermeldung:

```
LICENSE IS NOT VALID: java.io8.FileNotFoundException: C:\tenfold\license\tenfold.lic
(Das System kann die angegebene Datei nicht finden)
Product license invalid, stopping application server:
at.certex.ism.exception.ProductLicenseInvalidException: Product license is invalid!
```

Überprüfen Sie, ob eine Lizenzdatei im Ordner C:\tenfold\license\ vorhanden ist. Ist eine vorhanden, stellen Sie sicher, dass die Datei nicht beschädigt wurde, indem Sie sie erneut kopieren.

Ist die Datei nicht beschädigt, so kontrollieren Sie per SQL, ob die Default-Einstellung für die Lizenzdatei verändert wurde:

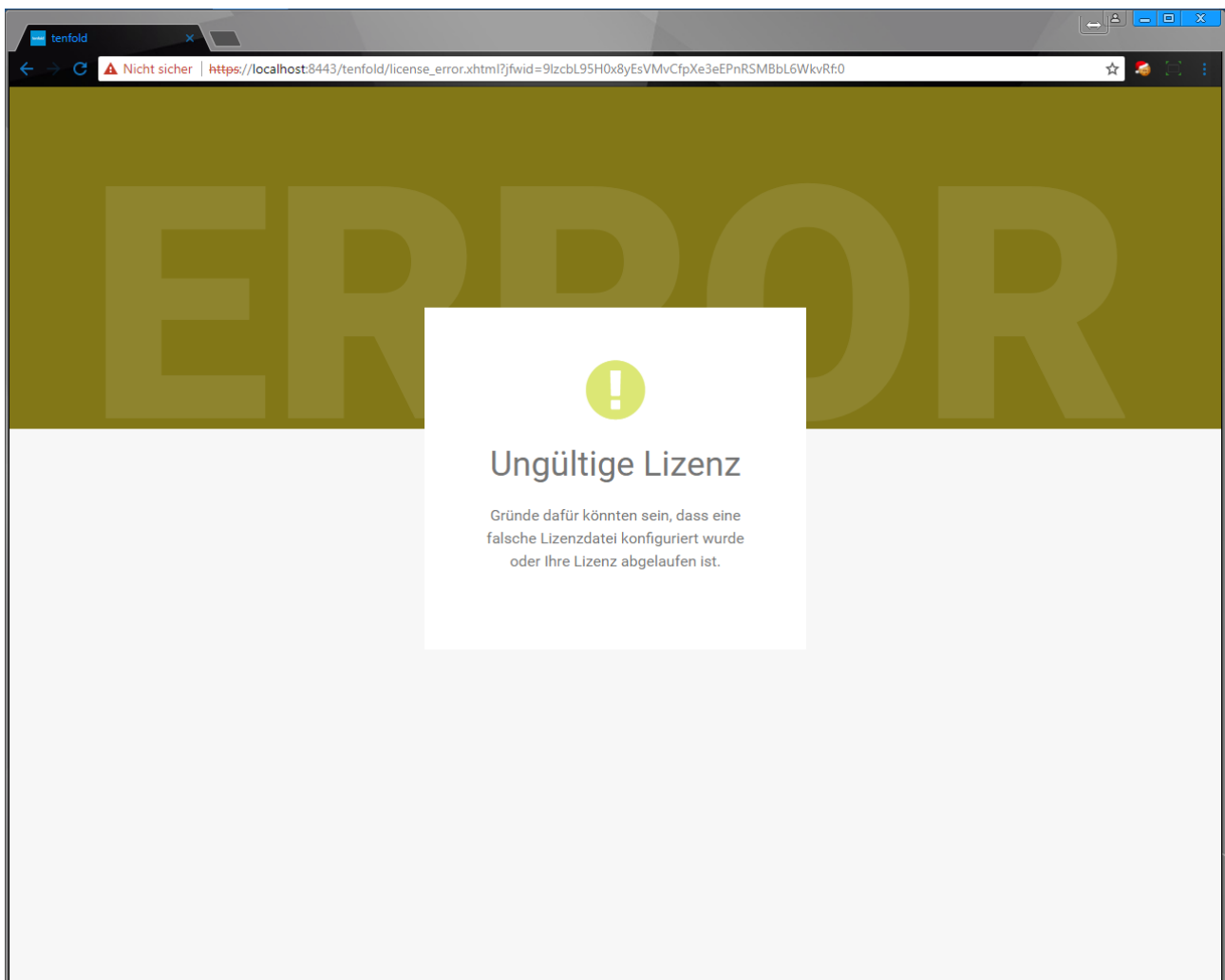
```
SELECT value FROM configuration WHERE name = 'license.file';
```

Wurde die Einstellung verändert, so kopieren Sie die Lizenzdatei an den neuen, dafür vorgesehenen Ort.

Lizenz abgelaufen

Ist die Lizenz abgelaufen, so startet der tenfold-Server normal, allerdings ist keine Anmeldung am System möglich. Sie erhalten stattdessen folgende Fehlermeldung:

⁸ <http://java.io/>

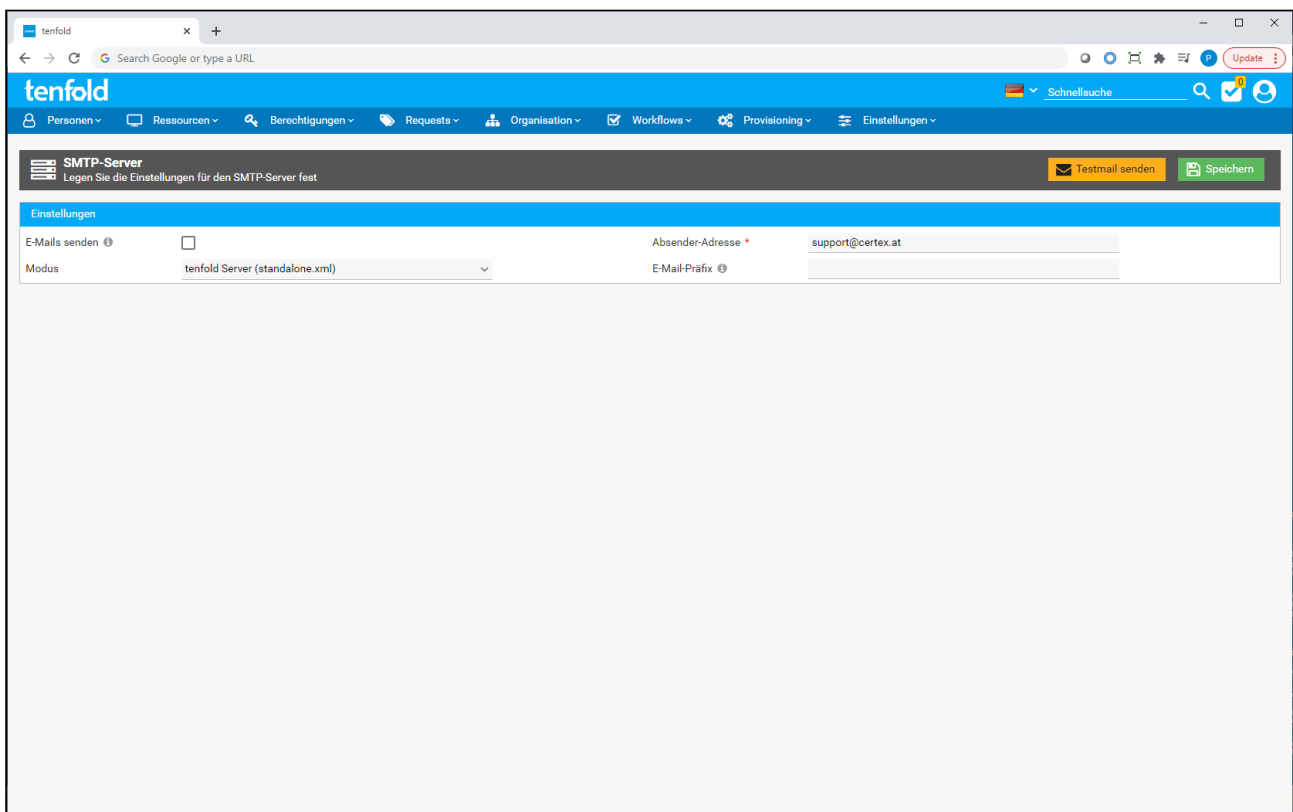


12.12 SMTP-Server

Erreichbar im Menü unter Einstellungen > E-Mail > SMTP-Server, kann auf dieser Maske konfiguriert werden, wie tenfold E-Mails versendet.

Benötigte Berechtigung

Für den Zugriff auf diese Seite wird die tenfold-Berechtigung "Notification administration"(8070) benötigt.



12.12.1 Allgemeine Einstellungen

Folgende Einstellungen werden unabhängig von der Einstellung Modus getroffen und bestimmen das Verhalten des E-Mail-Versandes.

Einstellung	Beschreibung
E-Mails senden	Ist diese Einstellung deaktiviert, sendet tenfold keine E-Mails. E-Mails welche gesendet würden, während diese Einstellung deaktiviert ist, erscheinen dennoch in der E-Mail Historie (siehe Historie gesendeter E-Mails (see page 536)). Ist diese Einstellung aktiviert, werden E-Mails ausgesendet.
Absender-Adresse	Hier kann eingestellt werden unter welcher Absender-Adresse tenfold E-Mails versenden soll.
E-Mail Präfix	Mit dieser Einstellung kann ein Text hinterlegt werden, welcher vor dem Betreff-Text aller gesendeten E-Mails beigefügt wird, ohne dies in jeder Vorlage extra machen zu müssen. Damit kann u.A. E-Mails die von tenfold gesendet werden leichter erkenntlich machen, indem man z.B. das Präfix "TF " vor die Betreffzeilen aller gesendeten E-Mails schreibt.

12.12.2 SMTP-Server Einstellungen

Die folgenden Einstellungen legen fest über welchen SMTP-Server tenfold E-Mails versendet. Zunächst ist folgende Einstellung tragend, welche definiert von welcher Quelle tenfold die SMTP-Server-Einstellungen bezieht.

Einstellung	Beschreibung
Modus	<p>Mit dieser Einstellung kann definiert werden, an welcher Stelle die SMTP-Serverkonfiguration festgelegt wird. Folgende zwei Optionen sind verfügbar:</p> <ul style="list-style-type: none"> • tenfold Server (standalone.xml) Ist diese Option ausgewählt, bezieht tenfold die Konfiguration des SMTP-Servers aus der tenfold Konfigurationsdatei im Installationsverzeichnis. Vor tenfold 2020 R4 Update 3 war dies der einzige Weg für die Konfiguration des SMTP-Servers. • Konfiguration Mit dieser Option, werden die Einstellungen in den tenfold Systemeinstellungen gespeichert und können daher direkt über die tenfold-Oberfläche bearbeitet werden.

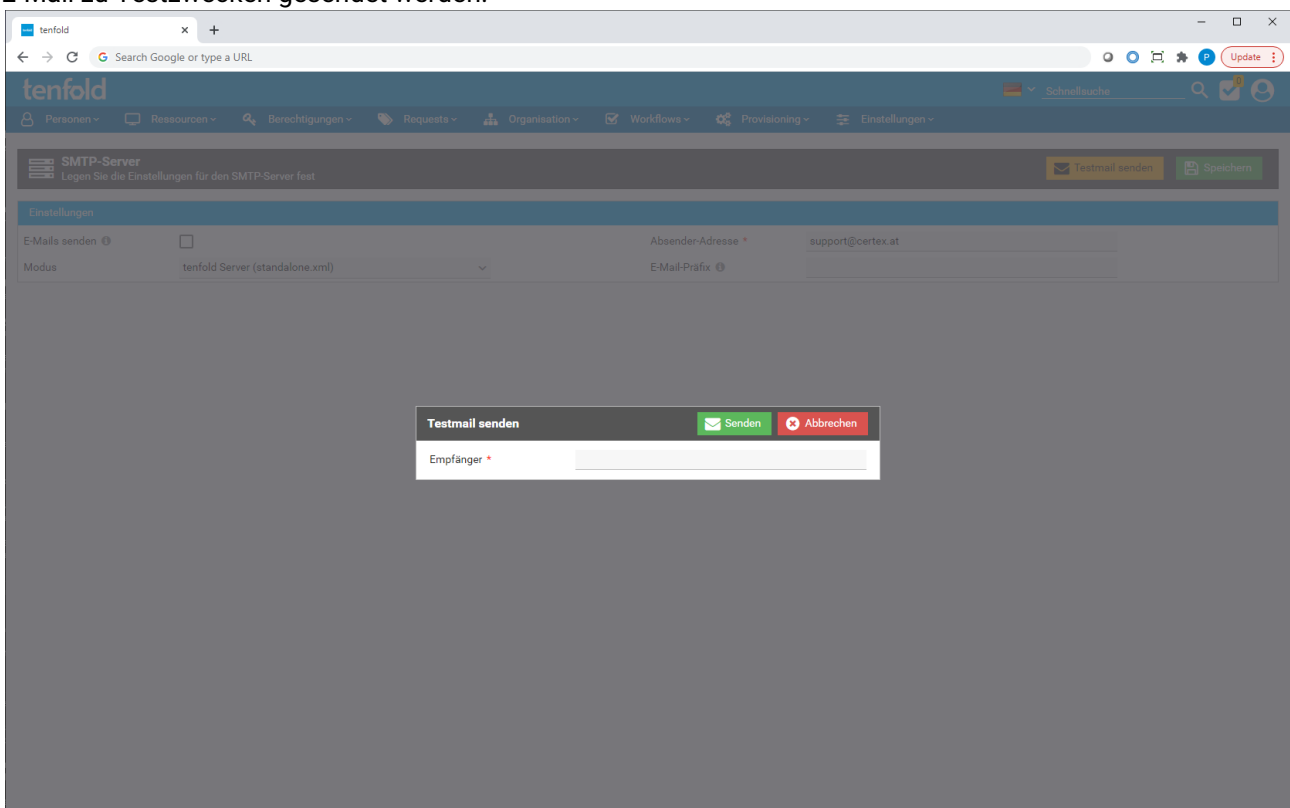
Wurde bei der Einstellung *Modus* der Wert *Konfiguration* gewählt, so werden neue Einstellungen auf der Maske sichtbar.

Einstellung	Beschreibung
Hostname	Mit dieser Einstellung wird der FQDN des SMTP-Servers festgelegt mittels welchem tenfold E-Mails versenden soll.
SMTP-Port	Der Netzwerk-Port auf welchem der SMTP-Server auf E-Mail-Anfragen horcht. Der Standardport für SMTP ist 25 (465 für TLS, 587 für StartTLS).

Einstellung	Beschreibung
Zugangsdaten	Erwartet der SMTP-Server eine Anmeldung zum Versenden von E-Mails, so können die Anmeldedaten hier hinterlegt werden. Zum Anlegen entsprechender Anmeldedaten siehe Zugangsdaten (see page 552).
Verbindungsmodus	Hier können Sie auswählen ob die Kommunikation mit dem SMTP-Server unverschlüsselt erfolgen soll oder mittels SSL oder StartTLS verschlüsselt werden soll.

12.12.3 Testmail senden

Um zu prüfen ob die getroffenen Einstellungen korrekt sind, kann mit der Schaltfläche Testmail senden eine E-Mail zu Testzwecken gesendet werden.



Im daraufhin erscheinenden Dialog geben Sie einfach den gewünschten Empfänger ein und klicken auf **Senden**. Daraufhin wird eine vordefinierte Testmail an die eingegebene Adresse gesendet. Ob die Nachricht erfolgreich war oder ob der Versand fehlgeschlagen ist, ist an einer Popup-Nachricht ersichtlich.

Vorlagen testen

Beachten Sie, dass diese Funktion dafür gedacht ist, zu prüfen ob mit den ausgewählten Einstellungen eine Kommunikation mit dem SMTP-Server möglich ist. Diese Funktion ist nicht dafür gedacht, spezifische Mailvorlagen auf Korrektheit zu prüfen.

12.13 Historie gesendeter E-Mails

Diese Maske dient dazu, die von tenfold gesendeten E-Mails zu prüfen und zu überwachen.

Benötigte Berechtigung

Für den Zugriff auf diese Seite wird die tenfold-Berechtigung "Notification administration"(8070) benötigt.

Gesendete E-Mails (11)
Zeigt E-Mails welche von tenfold gesendet wurden

Filter

Von: 01.09.2020
Bis: 29.01.2021
Status: -
Empfänger:
Text:

[Aktualisieren](#)

Datum	Empfänger	Vorlage	Sprache	Vertraulich	Status
25.11.2020 09:06:14		„Test	Englisch		AUSGESCHALTET MIT WARNUNGEN
30.10.2020 15:29:58	philip.markus@tenfold-security.com	Passwortempfänger	Englisch		AUSGESCHALTET
30.10.2020 15:29:56	philip.markus@tenfold-security.com	Active Directory Plugin - Windows Password	Englisch		AUSGESCHALTET
30.10.2020 15:29:54	lohnbuchhaltung@rv.de	„LRARV: Eintrittsdatum geändert	Englisch		AUSGESCHALTET
28.10.2020 15:41:21	irgendwer@irgendwo.de	Resource Provisioning - Default Notification	Englisch		AUSGESCHALTET
09.10.2020 15:28:18	philip.markus@tenfold-security.com	Passwortempfänger	Englisch		GESENDET
09.10.2020 15:28:17	philip.markus@tenfold-security.com	Active Directory Plugin - Windows Password	Englisch		GESENDET
09.10.2020 15:21:22	philip.markus@tenfold-security.com	Passwortempfänger	Englisch		GESENDET
09.10.2020 15:21:19	philip.markus@tenfold-security.com	Active Directory Plugin - Windows Password	Englisch		GESENDET
23.09.2020 09:48:58	test@test.com	Resource Provisioning - Default Notification	Englisch		GESENDET
23.09.2020 09:48:57	support@kunde.at	Resource Provisioning - Default Notification	Englisch		GESENDET

12.13.1 Allgemeine Informationen

Auf dieser Maske finden Sie eine Übersicht über alle von tenfold gesendeten E-Mails. Ausgenommen sind nur die Testmails der SMTP-Server-Maske. Diese werden **nicht** historisiert. Alle anderen E-Mails welche im Laufe der von tenfold durchgeführten Tätigkeiten gesendet werden, können hier aufgelistet, geprüft und im Bedarfsfall erneut gesendet werden.

Zeitraum der Historie

Der Zeitraum der einsehbaren Historie geht immer auf den Zeitpunkt der Installation von tenfold zurück. Eine automatisierte Bereinigung der Historie findet nicht statt.

Folgende Eigenschaften werden hier aufgelistet:

Spalte	Beschreibung
Datum	Datum und Uhrzeit zu welcher die E-Mail gesendet wurde.

Spalte	Beschreibung
Empfänger	Die Mailadresse an welche tenfold die E-Mail gesendet hat.
Vorlage	Die Textvorlage welche tenfold zum Erzeugen des Mailtextes verwendet hat.
Sprache	Die Sprache in welcher tenfold die E-Mail versendet hat.
Vertraulich	Zeigt an, ob die Textvorlage als vertraulich gekennzeichnet wurde. Texte von E-Mails mit vertraulichen Vorlagen werden in der Historie nicht gespeichert. Dies gilt im Regelfall für E-Mails, welche Passwörter beinhalten.
Status	Der Status der Sendung.

Es folgt eine Beschreibung der möglichen Status welche eine Sendung haben kann:

Status	Beschreibung
Gesendet	Die E-Mail wurde erfolgreich gesendet. Da nicht zustellbare E-Mails in der Regel durch Antwortmails quittiert werden und nicht durch eine Fehlermeldung des SMTP-Servers, kann tenfold an dieser Stelle nicht erkennen, dass die E-Mail nicht korrekt angekommen ist und wird diese E-Mail als erfolgreich gesendet markieren.
Gesendet mit Warnungen	Dieser Status entspricht dem Status <i>Gesendet</i> , jedoch wurden während der Erzeugung des Textes Warnungen erzeugt. Warnungen entstehen am häufigsten dadurch, dass Variablen in der Textvorlage nicht korrekt aufgelöst werden konnten.
Ausgeschaltet	Dies bedeutet, dass die E-Mail gesendet wurde, während das Senden von E-Mails global deaktiviert war (siehe SMTP-Server (see page 532)). Die E-Mail wurde dann zwar nicht gesendet, erscheint aber trotzdem unter diesem Status in der Historie. Dieser Status gibt keine Aussage darüber ob die Sendung erfolgreich gewesen wäre.
Ausgeschaltet mit Warnungen	Dies entspricht dem Status <i>Ausgeschaltet</i> , jedoch wurden während der Erzeugung des Textes Warnungen generiert. Warnungen entstehen am häufigsten dadurch, dass Variablen in der Textvorlage nicht korrekt aufgelöst werden konnten.
Fehler	Beim Senden der E-Mail ist ein Fehler aufgetreten. Dies kann entweder an einem schwerwiegenden Fehler beim Generieren des Mailtextes liegen oder an einem Fehler beim Versand. Genauere Informationen zu dem Fehler können in der Detailsicht (Aktion <i>Anzeigen</i>) eingesehen werden.

Die Ergebnismenge der angezeigten E-Mails lässt sich durch folgende Filtereinstellungen beeinflussen:

Einstellung	Beschreibung
Von	Hier wird das Datum angegeben, ab welchem gesendete E-Mails angezeigt werden. Die Uhrzeit ist dabei immer auf den Beginn des Tages gelegt (00:00:00). Wenn Sie die Maske betreten ist dieses Datum auf 1 Woche in der Vergangenheit gesetzt.
Bis	Hier wird das Datum angegeben, bis zu welchem gesendete E-Mails angezeigt werden. Die Uhrzeit ist dabei immer auf das Ende des Tages gelegt(23:59:59). Wenn Sie die Maske betreten ist dieses Datum auf das aktuelle Datum vorbelegt.
Status	Mit diesem Filter werden nur E-Mails im ausgewählten Status angezeigt.
Empfänger	Nur E-Mails deren Empfängerzeile den hier eingegebenen Text enthält werden angezeigt.
Text	Nur E-Mails deren Inhalt den hier eingegebenen Text enthält werden angezeigt.

12.13.2 Anzeige gesendeter E-Mails

The screenshot shows the 'E-Mail Logeintrag' (Email Log Entry) section in the tenfold application. It displays the details of a sent email. The table below summarizes the key information shown in the interface:

Daten			
Datum	23.09.2020 09:48:58	Vorlage	Resource Provisioning - Default Notification
Titel	Resource provisioning	Sprache	Englisch
Empfänger	test@test.com	Status	✓ GEGESendet
Vertraulich	-		

Below the table, the email content is displayed in a preview window. The content is a resource provisioning notification. The text of the notification is as follows:

Dear User,
The person ~~XXXXXXXXXX~~ has been assigned the resource ~~XXXXXXXXXX~~.
Once you have completed the required tasks, please click on the following link:
[Close](#)
Kind regards,
tenfold

At the bottom of the preview window, a small note states: "This is an automatically generated email, please do not reply to this message."

Durch die Aktion *Anzeigen* im Aktionsmenü der E-Mailliste gelangen Sie in eine Detailansicht der gesendeten Mail. Hier können Sie den Inhalt der E-Mail einsehen (sofern diese nicht als vertraulich markiert ist), oder mehr Details zu etwaigen Fehlermeldungen/Warnungen einsehen.
Es gibt 3 Karteireiter für die Ansicht der E-Mail.

Karteireiter	Beschreibung
HTML-Ansicht	Zeigt die E-Mail grafisch so an, wie Sie der Empfänger erhalten hat, sofern die E-Mail HTML-basiert ist. Handelt es sich um eine reine Textmail, ist dieser Reiter deaktiviert. Sie können die E-Mail zur übersichtlicheren Darstellung auch mit der entsprechenden Schaltfläche in einem neuen Browserfenster öffnen.
Text	Im Falle einer Textmail findet sich hier der normale gesendete Text wieder. Sollte es sich um eine HTML-Mail handeln wird der dahinterliegende Quelltext angezeigt.
Fehler/Warnungen	Im Fehlerfall wird hier eine detaillierte Meldung inklusive Stacktrace ausgegeben. Senden Sie in Fehlerfällen diese Fehlermeldung an Ihren Support damit dieser Sie effizienter unterstützen kann. Im Falle von Warnungen, werden diese ebenfalls in diesem Reiter angezeigt.

12.13.3 Erneutes Senden von E-Mails

Mit der Aktion *Erneut senden* im Aktionsmenü der Übersicht oder der Titelleiste der Detailanzeige können gesendete E-Mails erneut gesendet werden. Sie können diese Funktion benutzen um z.B. E-Mails erneut zu senden, deren Sendung aufgrund eines Ausfalles des SMTP-Servers fehlschlug.

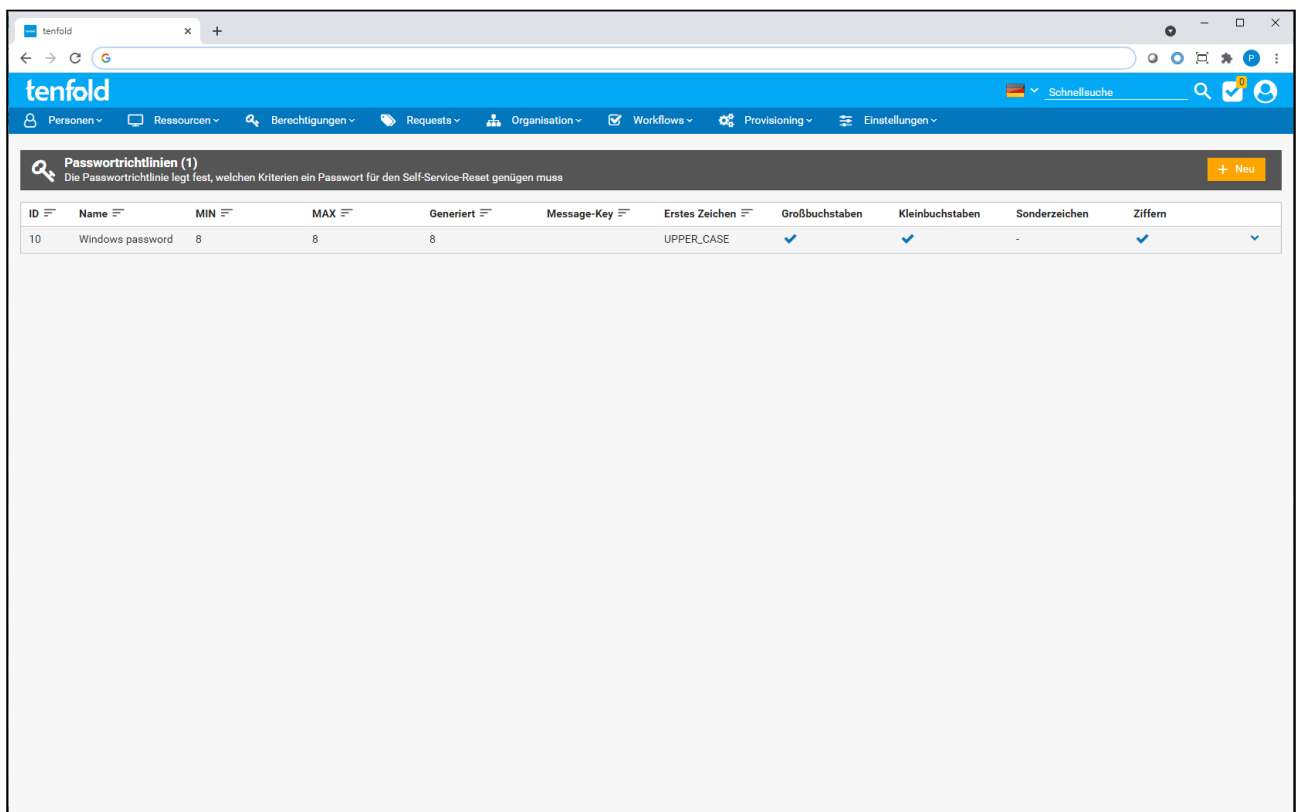
Keine Neugenerierung

Der Inhalt der E-Mail wird nicht neu erzeugt. Es wird der Inhalt, der damals erzeugt wurde exakt so wie er war erneut übermittelt. Eine Änderung der Vorlage hat daher keine Auswirkung auf den Inhalt erneut gesendeter E-Mails.

12.14 Passwortrichtlinien

Passwortrichtlinien stellen Regelwerke für Passwörter dar, welche zu zwei grundlegenden Zwecken verwendet werden:

- Überprüfung eingegebener Passwörter auf einen Mindeststandard
- Erzeugung zufälliger Passwörter



Benötigte Berechtigung

Für die Verwaltung ist die Systemberechtigung "Manage Password Policy" (8086) erforderlich.

Um die Passwortrichtlinien zu verwalten, navigieren Sie im Menü zur Maske *Einstellungen* > *Richtlinien* > *Passwortrichtlinien*. Sie gelangen daraufhin zur Maske mit der Übersicht aller bisher erstellten Passwortrichtlinien.

12.14.1 Erstellen und Bearbeiten von Passwortrichtlinien

Klicken Sie auf der Übersichtsmappe auf die Schaltfläche "Neu", um eine neue Richtlinie zu erstellen oder im Aktionsmenü der jeweiligen Richtlinie auf die Aktion "Bearbeiten", um Richtlinien zu ändern.

Neue Passwortrichtlinie bearbeiten
Erfassen Sie die gewünschten Stammdaten

[Passwort-Vorschau](#) [Speichern](#) [Abbrechen](#)

Einstellungen	Zeichen
Name *	Großbuchstaben <input type="checkbox"/>
Message-Key für die Beschreibung ⓘ	Kleinbuchstaben <input type="checkbox"/>
Minimale Länge * 3 ^	Sonderzeichen ⓘ <input type="checkbox"/>
Maximale Länge * 5 ^	Ziffern <input type="checkbox"/>
Generierte Länge * 5 ^	Leicht verwechselbare Zeichen ausschließen ⓘ <input type="checkbox"/>
Erstes Zeichen Beliebiges Zeichen ^	Ausgenommene Zeichen ⓘ

Folgende Einstellungen lassen sich bei einer Passwortrichtlinie einstellen, um festzulegen, wie anhand dieser Richtlinie Passwörter validiert oder generiert werden:

Einstellung	Beschreibung
Bereich "Einstellungen"	
Name	Legt den Namen der Passwortrichtlinie fest. Dieser Name dient zur Anzeige auf Masken in tenfold.
Message-Key für die Beschreibung	Mit dieser Einstellung legen Sie fest, welche Übersetzung verwendet wird, um beim Zurücksetzen eines Passwortes, in tenfold oder im Passwortportal, eine Hinweismeldung anzuzeigen, welche die Mindestanforderungen des Passwortes erläutert.
Minimale Länge	Legt fest, wie lange Passwörter, dieser Richtlinie zufolge, mindestens sein müssen.
Maximale Länge	Legt fest, wie lange Passwörter, dieser Richtlinie zufolge, höchstens sein dürfen.
Generierte Länge	Legt fest, wie lange Passwörter sein sollen, die nach dieser Richtlinie generiert werden.
Erstes Zeichen	Mit dieser Einstellung kann festgelegt werden, mit welcher Art von Zeichen ein Passwort beginnen muss.

Bereich "Zeichen"	
Großbuchstaben	Ist diese Einstellung aktiviert, müssen Passwörter, dieser Richtlinie zufolge, mindestens einen Großbuchstaben enthalten.
Kleinbuchstaben	Ist diese Einstellung aktiviert, müssen Passwörter, dieser Richtlinie zufolge, mindestens einen Kleinbuchstaben enthalten.
Sonderzeichen	Ist diese Einstellung aktiviert, müssen Passwörter, dieser Richtlinie zufolge, mindestens ein Sonderzeichen enthalten. Folgende Sonderzeichen werden unterstützt: -, / % \$ () _ < > ! ? # + = &
Ziffern	Ist diese Einstellung aktiviert, müssen Passwörter, dieser Richtlinie zufolge, mindestens eine Ziffer enthalten.
Leicht verwechselbare Zeichen ausschließen	Ist diese Einstellung aktiviert, so enthalten Passwörter, die nach dieser Richtlinie generiert wurden, niemals die folgenden Zeichen: 0 (Ziffer Null), O (Großbuchstabe o), l (Kleinbuchstabe L), 1 (Ziffer 1), (Pipe-Symbol), \$ (Dollarzeichen), § (Paragraphen-Zeichen). Diese Einstellung hat keine Auswirkung auf die Validierung eingegebener Passwörter.
Ausgenommene Zeichen	Legen Sie hier eine Reihe von Zeichen fest, welche bei der Erzeugung von Passwörtern, dieser Richtlinie zufolge, nicht verwendet werden dürfen. Diese Einstellung hat keine Auswirkung auf die Validierung eingegebener Passwörter.

Mindestanforderung bei der Erzeugung von Passwörtern

Beachten Sie, dass die Einstellungen "Großbuchstaben", "Kleinbuchstaben", "Sonderzeichen" und "Ziffern" die **Mindestanforderung** für generierte Passwörter darstellen. Dies bedeutet, dass generierte Passwörter zum Beispiel auch dann Ziffern enthalten können, wenn die Einstellung "Ziffern" nicht angehakt ist. Es wird lediglich garantiert, dass Passwörter, Ziffern enthalten, wenn die Einstellung "Ziffern" angehakt ist.

Wenn Sie mit den Einstellungen zufrieden sind, können Sie durch Betätigung der Schaltfläche "Passwort Vorschau" ein Passwort nach dieser Richtlinie generieren lassen. Das erzeugte Passwort wird Ihnen in einem Notiz-Popup angezeigt.

tenfold | Schnellsuche

Personen | Ressourcen | Berechtigungen | Requests | Organisation | Workflows | Provisioning | Einstellungen

Neue Passwortrichtlinie bearbeiten
Erfassen Sie die gewünschten Stammdaten

Einstellungen

Name *

Message-Key für die Beschreibung ⓘ

Minimale Länge *

Maximale Länge *

Generierte Länge *

Erstes Zeichen

Zeichen

Großbuchstaben ☒

Kleinbuchstaben ☒

Sonderzeichen ⓘ ☐

Ziffern ☒

Leicht verwechselbare Zeichen ausschließen ⓘ ☐

Ausgenommene Zeichen ⓘ

Das generierte Passwort lautet:
K7AQa7WhBFR

Klicken Sie auf die Schaltfläche "Speichern", um die getroffenen Änderungen zu speichern.

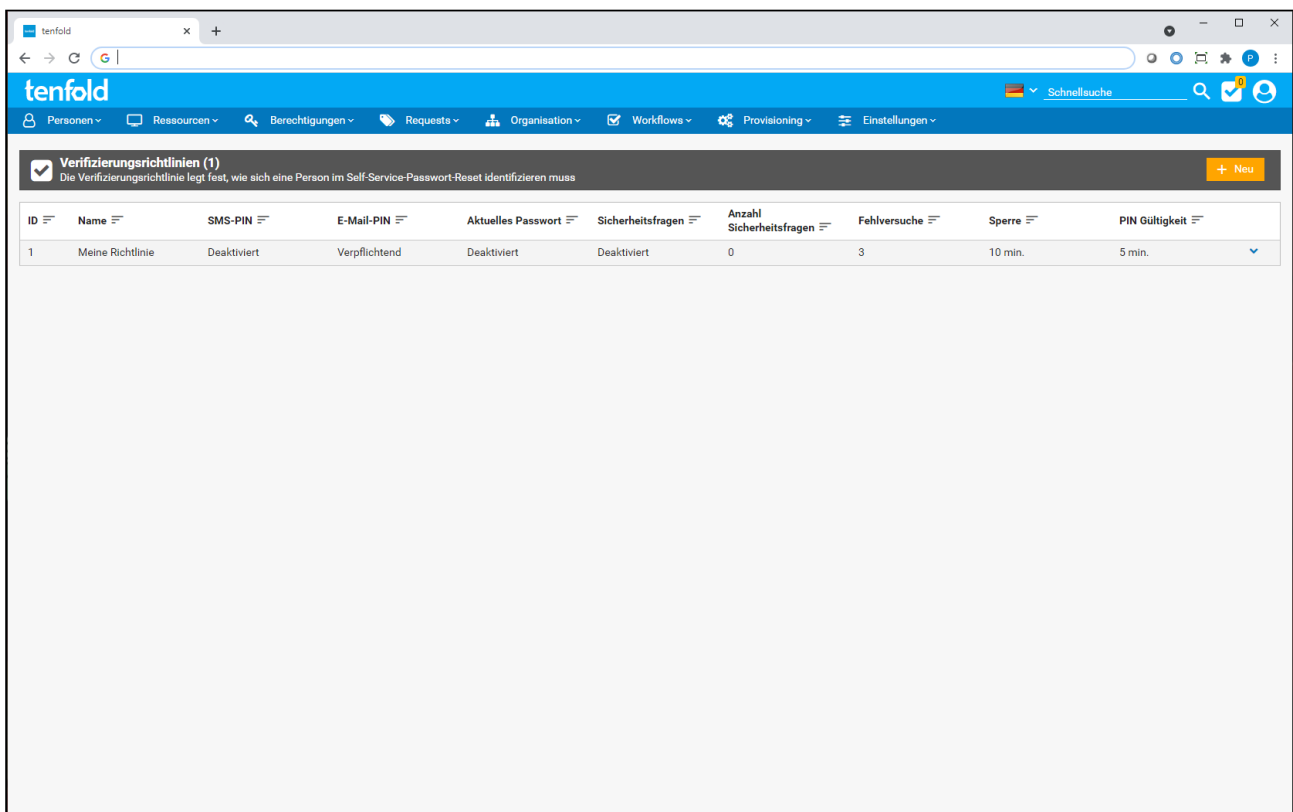
12.14.2 Passwortrichtlinien anwenden

Passwortrichtlinien kommen überall dort zum Einsatz, wo Passwörter erzeugt werden oder wo Passwörter auf eine gewisse Qualität geprüft werden müssen.

Sie können zum Beispiel für jede Personenart (siehe [Personenarten](#)(see page 81)) festlegen, welche Passwortrichtlinie für den Passwort-Reset zum Tragen kommt. Hierbei kann die Richtlinie entweder dazu verwendet werden, Benutzerpasswörter zu validieren oder um Passwörter automatisch generieren zu lassen. Darüber hinaus erlauben es die verschiedenen Plugins, die Benutzerkonten anlegen, Passwortrichtlinien zu hinterlegen, um mit diesen Passwörter für neu angelegte Konten zu erzeugen. Siehe [Erzeugung von Passwörtern](#)(see page 648) für mehr Informationen hierzu.

12.15 Verifizierungsrichtlinien

Passwörter stellen die primäre Form der Authentifizierung dar, mit welcher Benutzer ihre Identität beweisen können. Es kommt jedoch häufig vor, dass Benutzer ihre Passwörter vergessen. Damit die Passwörter sicher zurückgesetzt werden können, bedarf es in solchen Fällen einer alternativen Methode, um die Identität von Benutzern zu gewährleisten.



12.15.1 Allgemeines

Der Umgang mit verloren gegangenen Passwörtern ist ein heikles Thema. Auf der einen Seite sollte es der IT schnell und einfach möglich sein, Passwörter zurückzusetzen; auf der anderen Seite muss ein Missbrauch dieser Funktion verhindert werden. In der Regel gibt es zwei Vorgangsweisen, um verlorene Passwörter zurückzusetzen:

1. Der Benutzer hat das Passwort zu seinem Systemzugang vergessen und kommt gar nicht mehr in seinen PC. Er benötigt Unterstützung der IT (eventuell telefonisch), um sein Kennwort zurückzusetzen.
2. Der Benutzer hat ein Passwort zu einer Anwendung vergessen, hat jedoch noch Zugang zu seinem PC und möchte sein Passwort selbst zurücksetzen.

In beiden Fällen ist es notwendig, dass der Benutzer die Korrektheit seiner Identität beweist, um zu verhindern, dass ungewollt fremde Passwörter zurückgesetzt werden. Mit den Verifizierungsrichtlinien in tenfold legen Sie Schemen fest, mit welchen der Benutzer seine Identität, für beide dieser Szenarien, beweisen kann.

12.15.2 Verwaltung von Verifizierungsrichtlinien

Benötigte Berechtigung

Für die Verwaltung ist die Systemberechtigung "Manage Verification Policies" (8087) erforderlich.

Um die Verifizierungsrichtlinien in tenfold zu verwalten, navigieren Sie im Menü zu *Einstellungen > Richtlinien > Verifizierungsrichtlinien*. Damit gelangen Sie auf die Übersichtsmaske der vorhandenen Verifizierungsrichtlinien. Klicken Sie auf die Schaltfläche "Neu", um eine neue Verifizierungsrichtlinie

anzulegen oder wählen Sie die Aktion "Bearbeiten" im Aktionsmenü, um eine bestehende Richtlinie zu bearbeiten.

The screenshot shows the 'Verifizierungsrichtlinie bearbeiten' (Edit Verification Policy) page in the tenfold web application. The page has a blue header with the tenfold logo and navigation menu. The main content area is titled 'Verifizierungsrichtlinie bearbeiten' and includes a subtitle 'Erfassen Sie die gewünschten Stammdaten'. There are two buttons: 'Speichern' (Save) and 'Abbrechen' (Cancel). The form is divided into several sections:

- Verifizierungsrichtlinie**: Contains fields for 'Name' (Meine Richtlinie), 'Fehlversuche' (3), 'Sperre' (10 Minuten), and 'Groß-/Kleinschreibung ignorieren' (checkbox).
- PIN-Verifizierung**: Includes a sub-section for 'E-Mail' with fields for 'Richtlinie' (Verpflichtend), 'Modus' (Konfiguration), 'Vorlageneinstellung' (Standardvorlage verwenden), 'Empfänger' (Auswahl Personenfeld), and 'Personenfeld' (E-Mail). There is also a sub-section for 'SMS' with 'Richtlinie' (Deaktiviert) and a sub-section for 'PIN Gültigkeit' with 'Dauer' (5 Minuten).
- Sicherheitsfragen**: Includes a field for 'Sicherheitsfragen' (Deaktiviert).
- Active Directory-Password**: Includes a field for 'Aktuelles Passwort' (Deaktiviert).

Verifizierungsrichtlinien unterstützen folgende Verifizierungsmethoden:

- PIN-Codes
- Sicherheitsfragen
- Active-Directory-Password

Die möglichen Einstellungen dazu werden in den folgenden Abschnitten behandelt.

Allgemeine Einstellungen

Im Bereich "Verifizierungsrichtlinie" finden Sie folgende allgemeinen Einstellungen zu der Verifizierungsrichtlinie. Diese Einstellungen sind keiner bestimmten Verifizierungsmethode zugeordnet.

Einstellung	Beschreibung
Name	Der Name der Richtlinie. Dieser Name wird zur Anzeige auf Masken in tenfold verwendet.
Fehlversuche	Legt fest, wie viele Fehlversuche erlaubt sind, bevor tenfold die Authentifizierung für eine gewisse Zeit verweigert.
Sperre	Legt fest, wie lange die Authentifizierung gesperrt ist, sollten zu viele Fehlversuche stattgefunden haben.

Einstellung	Beschreibung
Groß-/Kleinschreibung ignorieren	Ist diese Einstellung aktiviert, so wird bei der Eingabe von PIN-Codes, Antworten auf Sicherheitsfragen, usw., die Groß- und Kleinschreibung nicht beachtet. Diese Einstellung hat keine Auswirkung auf die Abfrage des Active Directory Passwortes.

Fehlversuche und Sperre

Mit einer Sperrung ist in diesem Zusammenhang gemeint, dass tenfold weitere Authentifizierungsversuche, zum Zwecke der Zurücksetzung des Passwortes, für eine gewisse Zeit verweigert. Dies hat keine Auswirkung auf das Konto, zu welchem das Passwort gehört. Dieses wird hierbei nicht gesperrt.

PIN-Einstellungen

Folgende Einstellungen können zum Versand von PIN-Codes getroffen werden. PIN-Codes können entweder per E-Mail oder SMS versendet werden. PIN-Codes, auch Tokens genannt, sind eine Kombination von Ziffern und Buchstaben, welche an ein Gerät im Besitz der Person übermittelt werden können, damit diese ihre Identität bestätigen kann. Für die Übermittlung der Codes muss tenfold über die E-Mail-Adresse oder die Handynummer der Person verfügen.

Folgende Einstellungen hierzu sind im Bereich "PIN-Verifizierung" vorhanden:

Einstellung	Beschreibung
Abschnitt "E-Mail"	
Richtlinie	Legt fest, ob PIN-Codes/Tokens per E-Mail gesendet werden oder nicht. <ul style="list-style-type: none"> • Deaktiviert: Es wird kein Token gesendet. • Verpflichtend: Es wird ein Token gesendet. • Optional: Es wird ein Token gesendet, wenn tenfold die Zieladresse bekannt ist.
Modus	Legt fest, ob die Tokens mittels der folgend eingestellten Optionen gesendet werden soll oder ob der Legacy-EXEC "System.sendTokens" verwendet werden soll. Diese Einstellung ist nur von Bedeutung, wenn Sie von einer älteren Version von tenfold aktualisiert haben und der Versand der Tokens bereits mittels Legacy-EXEC gelöst wurde. Andernfalls behalten Sie die Einstellung "Konfiguration" bei.
Vorlageneinstellung	Legt fest, ob der Code mit der mitgelieferten Standardvorlage versendet werden soll oder ob Sie eine eigene Vorlage einsetzen möchten.
Vorlage	Hier legen Sie die Vorlage fest, mit welchem die Codes versendet werden sollen, wenn Sie im Feld "Vorlageneinstellung" die Option "Selbsterstellte Vorlage verwenden" ausgewählt haben.
Empfänger	Diese Einstellung legt fest, ob die Auswahl des Empfängers mittels eines Personenfeldes oder mittels eines Code Snippets erfolgen soll.

Personenfeld	Hier legen Sie das Personenfeld fest, welches zur Auswahl der Empfängeradresse benutzt wird. Ist dieses Feld leer und die Richtlinie als "Verpflichtend" markiert, so verweigert tenfold das Zurücksetzen des Passwortes bereits im Vorfeld.
Code Snippet	<p>Ein Code Snippet, das eine E-Mail-Adresse liefern muss, an die die Tokens gesendet werden können. Liefert dieses Snippet ein leeres Resultat und ist die Richtlinie als "Verpflichtend" markiert, so verweigert tenfold das Zurücksetzen des Passwortes bereits im Vorfeld.</p> <p>Folgende Parameter stehen Ihnen in diesem Snippet zur Verfügung:</p> <ul style="list-style-type: none"> • policy: Das VerificationPolicy-Objekt, welches diese Richtlinie darstellt. • person: Die Person, die verifiziert werden soll. • user: Die Person, die an tenfold angemeldet ist, um die Verifizierung durchzuführen. • wrapper: Alle bisher eingegebenen Daten. • mode: Eine Zeichenkette, welche entweder "PASSWORD" enthält, wenn die Verifizierung zur Zurücksetzung des Passwortes durchgeführt wird, oder "SETTINGS", wenn die Verifizierung zur Beantwortung der Sicherheitsfragen stattfindet.
Abschnitt "SMS"	
Richtlinie	<p>Legt fest, ob PIN-Codes mittels SMS gesendet werden oder nicht.</p> <ul style="list-style-type: none"> • Deaktiviert: Es wird kein Token gesendet. • Verpflichtend: Es wird ein Token gesendet. • Optional: Es wird ein Token gesendet, wenn tenfold die entsprechende Telefonnummer bekannt ist.
Modus	Legt fest, ob die Tokens mittels der folgend eingestellten Optionen gesendet werden soll oder ob der Legacy-EXEC "System.sendTokens" verwendet werden soll. Diese Einstellung ist nur von Bedeutung, wenn Sie von einer älteren Version von tenfold aktualisiert haben und der Versand der Tokens bereits mittels Legacy-EXEC gelöst wurde. Andernfalls behalten Sie die Einstellung "Konfiguration" bei.
Aktion	Mit der Einstellung "E-Mail" legen Sie fest, dass tenfold die Tokens mittels eines E-Mail Gateways versenden soll. Hierbei handelt es sich um spezielle Programme, welche eingehende E-Mails als SMS versenden. Beachten Sie, dass tenfold über keinen eigenen SMS-Gateway verfügt. Dieser muss anderweitig bereitgestellt werden. "Code Snippet" bedeutet, dass ein Code Snippet verwendet wird, um die SMS zu versenden.
Vorlageneinstellung	Haben Sie in dem Feld "Aktion" die Einstellung "E-Mail versenden" gewählt, so können Sie hier bestimmen, ob eine mitgelieferte Standardvorlage für den Versand verwendet werden soll oder ob Sie eine eigens definierte Vorlage verwenden möchten.

Vorlage	Mit dieser Einstellung können Sie die selbsterstellte Vorlage definieren, welche verwendet werden soll, wenn Sie im Feld "Vorlageneinstellung" den Wert "Selbsterstellte Vorlage verwenden" gewählt haben.
Code Snippet	<p>Definiert das Code-Snippet, welches dafür zuständig ist, den SMS-PIN zu erzeugen und zu versenden.</p> <p>Folgende Parameter werden an das Snippet übergeben</p> <ul style="list-style-type: none"> • person: Die Person, die verifiziert wird. • sms: Ein boolscher Wert, welcher angibt, ob SMS-Tokens versendet werden sollen. • mail: Ein boolscher Wert, welcher angibt, ob E-Mail-Tokens versendet werden sollen. • mailDestination: Die E-Mail-Adresse, an welche E-Mail-Tokens versendet werden sollen. • phoneDestination: Die Telefonnummer, an welche SMS-Tokens versendet werden sollen. • tokenStore: Eine Klasse, welche Informationen zu den bisher gesetzten Tokens enthält. <p>Dieses Snippet muss den erzeugten Token zurückliefern.</p>
E-Mail-Empfänger	<p>Legt fest, ob die Empfängeradresse fest hinterlegt wird oder durch ein Code Snippet bestimmt wird. SMS-Gateways funktionieren normalerweise auf eine von zwei Weisen:</p> <ul style="list-style-type: none"> • Die Telefonnummer wird durch die Empfängeradresse festgelegt (z.B. 123456@my-gateway.de) • Die Telefonnummer befindet sich in der E-Mail (meist in der Betreffzeile). <p>Sollte die Telefonnummer durch die Empfängeradresse bestimmt werden, wählen Sie "Code Snippet"; andernfalls wählen Sie "E-Mail".</p>
E-Mail	Die E-Mail-Adresse, an welche der SMS-Text gesendet werden soll. Diese Einstellung ist nur Verfügbar, wenn im Feld "E-Mail-Empfänger" die Auswahl "E-Mail" getroffen wurde.

Code Snippet	<p>Legt das Code Snippet fest, welches die Empfängeradresse für die SMS erzeugt.</p> <p>Folgende Parameter werden an das Snippet übergeben:</p> <ul style="list-style-type: none"> • person: Die Person, die verifiziert wird. • sms: Ein boolscher Wert, welcher angibt, ob SMS-Tokens versendet werden sollen. • mail: Ein boolscher Wert, welcher angibt, ob E-Mail-Tokens versendet werden sollen. • mailDestination: Die E-Mail-Adresse, an welche E-Mail-Tokens versendet werden sollen. • phoneDestination: Die Telefonnummer, an welche SMS-Tokens versendet werden sollen. • tokenStore: Eine Klasse, welche Informationen zu den bisher gesetzten Tokens enthält. <p>Das Snippet muss eine Empfängeradresse für den SMS-Gateway zurückliefern.</p>
SMS-Empfänger	<p>Legt fest, wie die Telefonnummer ermittelt wird, an welche die SMS gesendet werden soll. "Auswahl Personenfeld" legt fest, dass sich die Telefonnummer in einem definierten Personenfeld befinden muss. "Code Snippet" bedeutet, dass ein Code Snippet verwendet werden soll, welches die Telefonnummer liefert.</p>
Personenfeld	<p>Das Personenfeld, in welchem sich die Telefonnummer befindet. Ist dieses Personenfeld leer und die Richtlinie auf "Verpflichtend" gestellt, so verweigert tenfold die Authentifizierung bereits im Vorfeld. Diese Einstellung ist nur Verfügbar, wenn im Feld "SMS-Empfänger" die Auswahl "Auswahl Personenfeld" getroffen wurde.</p>
Code Snippet	<p>Ein Code Snippet, welches die Empfängernummer für den SMS-Token liefern muss. Liefert dieses Snippet ein leeres Resultat und ist die Richtlinie auf "Verpflichtend" gestellt, so verweigert tenfold die Authentifizierung bereits im Vorfeld.</p> <p>Folgende Parameter werden an das Snippet übergeben:</p> <ul style="list-style-type: none"> • policy: Das VerificationPolicy-Objekt, welches diese Richtlinie darstellt. • person: Die Person, welche verifiziert werden soll. • user: Die Person, welche an tenfold angemeldet ist, um die Verifizierung durchzuführen. • wrapper: Alle bisher eingegebenen Daten. • mode: Eine Zeichenkette, welche entweder "PASSWORD" enthält, wenn die Verifizierung zur Zurücksetzung des Passwortes durchgeführt wird oder "SETTINGS", wenn die Verifizierung zur Beantwortung der Sicherheitsfragen stattfindet. <p>Das Snippet muss die Telefonnummer liefern, an welche der Token gesendet werden soll.</p>

Abschnitt "PIN Gültigkeit"

Dauer

Die Dauer, in Minuten, für wie lange tenfold die gesendeten Tokens als gültig erachtet. Ist diese Zeit überschritten muss der Authentifizierungsversuch abgebrochen und erneut gestartet werden.

Verpflichtend/Optional

Im Zusammenhang mit der Verifizierungsmethode haben die Einstellungen "Verpflichtend" und "Optional" folgende Bedeutung:

- **Verpflichtend:** Ist die Methode verpflichtend, so verweigert tenfold ein Zurücksetzen des Passwortes, wenn tenfold nicht über ausreichend Informationen zu dieser Methode und Person verfügt. Zum Beispiel: Sind E-Mail-PINs als "Verpflichtend" ausgewählt, so muss tenfold die E-Mail-Adresse der Person kennen. Andernfalls verweigert tenfold dieser Person das Zurücksetzen des Passwortes.
- **Optional:** tenfold fordert nur dann diese Verifizierungsmethode an, wenn tenfold über genügend Informationen verfügt. Zum Beispiel: E-Mail-PINs sind als "Optional" eingestellt. Ist tenfold die E-Mail-Adresse der Person bekannt, wird tenfold einen PIN an diese Adresse senden und diese auch abfragen. Ist die E-Mail-Adresse unbekannt, überspringt tenfold diese Verifizierungsmethode.

Bei der Verifizierung sind verpflichtend markierte Felder immer einzutragen. Sollte es nur optionale Felder geben, so ist **zumindest eines** davon anzugeben.

Sicherheitsfragen

Sicherheitsfragen sind Fragen, welche in tenfold hinterlegt werden und im Vorfeld vom Benutzer beantwortet werden müssen. Sobald der Benutzer die Antworten für die Fragen hinterlegt hat, kann die Identität durch korrekt Antworten sichergestellt werden.

Social Engineering

Es wird empfohlen, beim Eintragen der Antworten zu lügen oder passwortähnliche Antworten zu geben. Dies hat den Vorteil, dass fremde Personen, welche über das richtige Wissen verfügen, nicht die Möglichkeit erhalten, die Passwörter einer anderen Person zurücksetzen zu können. Da nicht davon auszugehen ist, dass Ihre Benutzer dies auch tun, sollten Sie die Sicherheitsfragen so wählen, dass sie sich nicht einfach social engineeren lassen.

Folgende Einstellungen können zu dieser Identifikationsmethode im Bereich "Sicherheitsfragen" getroffen werden.

Einstellung	Beschreibung
Sicherheitsfragen	Legen Sie hier fest, ob Sicherheitsfragen erforderlich sind oder nicht.

Einstellung	Beschreibung
Berechtigung zur Anzeige der Antworten	Legt eine tenfold-Berechtigung fest, welche es dem Benutzer erlaubt, bei der Beantwortung der Fragen die richtigen Antworten einzublenden. Dies kann für den Helpdesk notwendig sein, welcher Passwörter durch Telefonanfragen zurücksetzen soll. Im Falle von komplizierten Antworten kann es dann daran scheitern, dass der Helpdesk die Antworten nicht vollständig korrekt eingibt, obwohl die richtigen Antworten gegeben werden.
Berechtigung für das Einrichten von Fragen	Diese Einstellung legt fest, welche tenfold-Berechtigung benötigt wird, um die eigenen Sicherheitsfragen zu beantworten. Ohne dieser Berechtigungen können keine Sicherheitsfragen hinterlegt werden. Sind Sicherheitsfragen als "Verpflichtend" eingestellt, so können Personen ohne diese Berechtigung ihr Kennwort nicht zurücksetzen.
Anzahl Sicherheitsfragen	Legt fest, wie viele der eingegebenen Sicherheitsfragen zur erfolgreichen Identifizierung beantwortet werden müssen.

Active Directory-Passwort

Mit der Einstellung im Bereich "Active Directory-Passwort" wird festgelegt, ob die Identifizierung das aktuelle Windows-Passwort des Benutzers voraussetzt.

Das Passwort wurde doch vergessen

Diese Einstellung bezieht sich speziell auf das Active Directory-Passwort des Benutzers und nicht auf das Passwort, das zurückgesetzt werden soll. Mit dieser Einstellung kann, zum Beispiel, erreicht werden, dass ein Benutzer mithilfe seines Active Directory-Passwortes, ein Passwort aus einem anderen System (z.B. SAP) zurücksetzen kann.

Es wird empfohlen, in der Verifizierungsrichtlinie, die erforderlich ist, um die Sicherheitsfragen zu beantworten, das Active Directory-Passwort mit einzubeziehen.

Einmalpasswort

Mit dieser Einstellung wird geregelt, ob Personen ihr Einmalpasswort (2-Faktor-Authentifizierung) angeben müssen. Hierfür benötigt die Person die Berechtigung "Two Factor Authentication" (8500) und muss bei der ersten Anmeldung darauf einen Google Authenticator mit tenfold verbinden. Sobald dies geschehen ist, kann dieser Authenticator auch beim Zurücksetzen des Passwortes mittels dieser Einstellung verwendet werden. Bei der Identifizierung muss dann der aktuelle Token, welcher in der Google Authenticator App angezeigt wird, eingegeben werden.

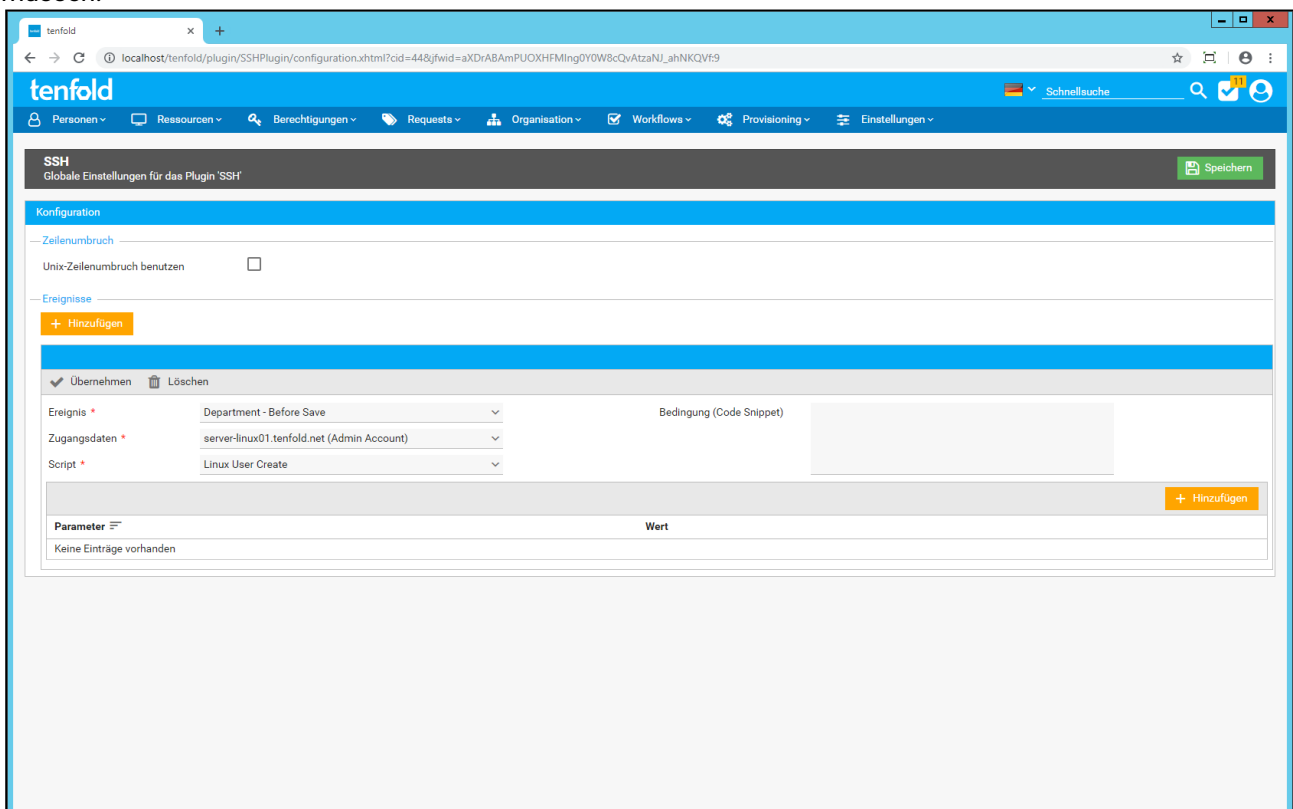
13 Provisioning

13.1 Zugangsdaten

13.1.1 Allgemeines

Die Funktion Zugangsdaten dient der Speicherung und Verwaltung von Verbindungsdaten und Benutzernamen und Passwörtern für die Verbindung zu Zielsystemen. Üblicherweise wird zum Verbindungsaufbau zu einem Zielsystem ein administratives Benutzerkonto benötigt, welches die gewünschten Aktionen über die Verbindungsschnittstelle auslösen kann. Diese administrativen Informationen werden in der Funktion "Zugangsdaten" zentral verwaltet. Die unterschiedlichen hinterlegten Zugangsdaten können dann unter der gewählten Bezeichnung für die unterschiedlichen Verbindungen (zumeist als Einstellung in Plugins) ausgewählt werden.

Der nachfolgende Screenshot zeigt, wie die Zugangsdaten im Rahmen des SSH Plugin ausgewählt werden müssen.

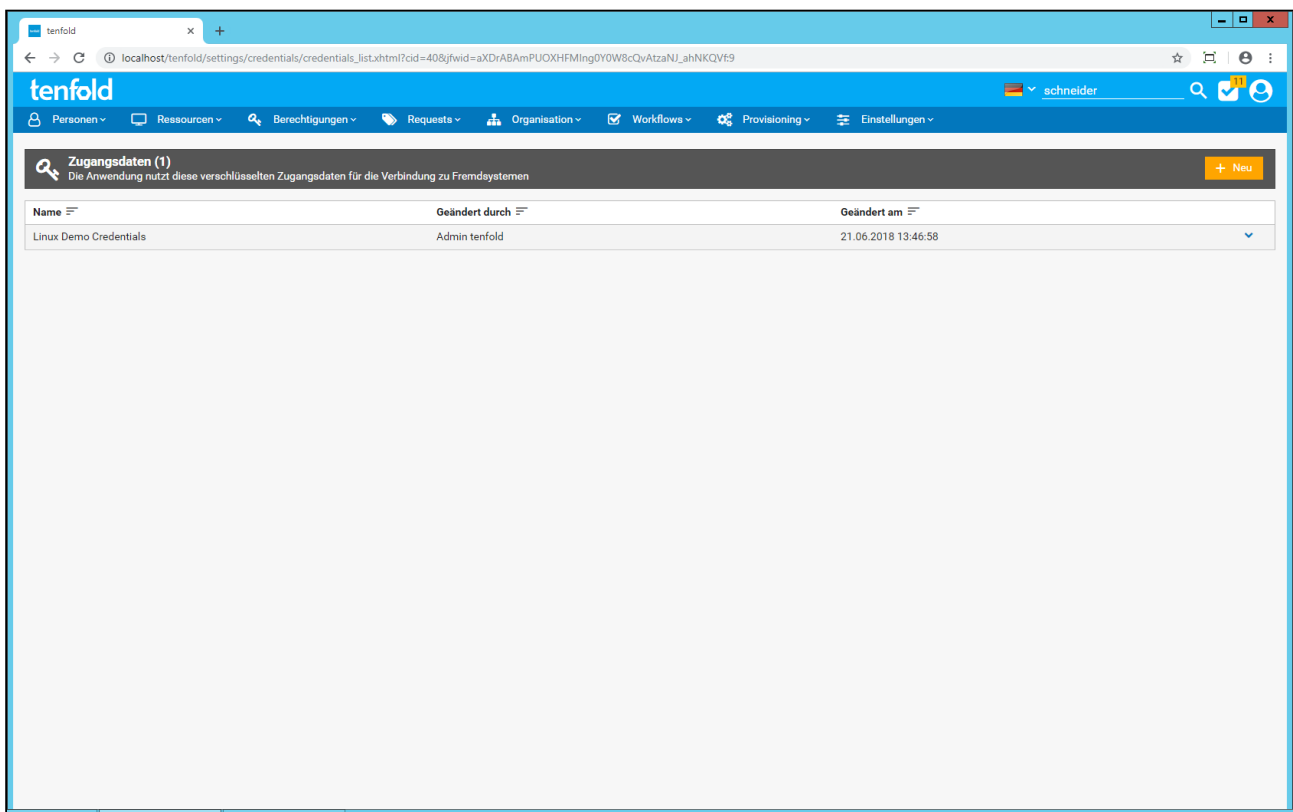


13.1.2 Verwaltung

Die Funktion ist über das Menü > Provisioning > Zugangsdaten erreichbar.

Benötigte Berechtigung

Für die Verwaltung ist die Systemberechtigung "Manage Credentials" (8085) erforderlich.



Die Maske zeigt alle hinterlegten Zugangsdaten an. Neue Einträge können mit dem Button "Neu" angelegt werden. Hierbei muss aus einer Dropdown-Liste der Typ der anzulegenden Zugangsdaten angegeben werden. Verschiedene Typen von Zugangsdaten verfügen über verschiedene Felder, welche, zusätzlich zu den Zugangsdaten, eingegeben werden können. Einmal angelegt, kann der Typ der Zugangsdaten nicht mehr verändert werden. Folgende Arten von Zugangsdaten können standardmäßig angelegt werden.

Zugangsdatenart	Beschreibung
Standard	Diese Art von Zugangsdaten verfügt über zwei generische Parameter: Verbindung 1, Verbindung 2. Dieser Typ wird von tenfold-Funktionen oder für Plugins verwendet, welche neben den Zugangsdaten keine weiteren Parameter benötigen und daher keinen eigenen Typen definieren. Die Parameter Verbindung 1, oder Verbindung 2 können dennoch, zum Beispiel in Skripten, benutzt werden.
Exchange EWS	Zugangsdaten, welche für die Exchange-Server-Konfiguration verwendet werden. (Siehe Einrichtung der Exchange Server (see page 233))
Exchange PowerShell	Zugangsdaten, welche für die Exchange-Server-Konfiguration verwendet werden. (Siehe Einrichtung der Exchange Server (see page 233))
JDBC	Zugangsdaten, welche für Java-Datenbankverbindungen benutzt werden können. Diese wird, zum Beispiel, vom Import Plugin benutzt, wenn die Datenquelle eine Datenbank ist.
SMTP	Wird verwendet um Zugangsdaten für die Anmeldung an SMTP-Servern zu ermöglichen. (Siehe SMTP-Server (see page 532))

Plugins

Zusätzlich zu den hier aufgeführten Arten von Zugangsdaten, können Plugins bei der Installation oder bei Update weitere Typen hinzufügen.

Bestehende Einträge können im Kontextmenü über die Option "Bearbeiten" bearbeitet werden.
Bestehende Einträge können nur gelöscht werden, wenn sie sich nicht aktuell in Verwendung befinden.

13.1.3 Anlage und Bearbeitung

Folgende allgemeine Daten können zu einem Eintrag eingegeben werden, unabhängig vom gewählten Zugangsdatentyp:

Feld	Beschreibung
Name	Der Name des Datensatzes. Dieser wird in Auswahlfeldern auf tenfold-Masken angezeigt.
Benutzername	Der Benutzername, der für die Verbindung verwendet werden soll.
Passwort	Das Passwort, welches für den Verbindungsaufbau genutzt werden soll.
Bestätigung	Die Wiederholung des oben angegebenen Passwortes.

Bedeutung von Verbindung 1/2

Die beiden Felder *Verbindung 1* und *Verbindung 2* sind Einstellungen welche bei der Zugangsdatenart "Standard" vorhanden sind. Diese stellen allgemeine Verbindungsparameter dar, welche in unterschiedlichen

Kontexten unterschiedlich verwendet werden können. Normalerweise wird die Verbindungsart "Standard" verwendet, wenn es für kleinere Anpassungen (z.B. das Anbinden von PowerShell-Skripten) notwendig ist, Zugangsdaten in tenfold zu hinterlegen.

Standardanbindungen (z.B. OTRS, Microsoft SQL Server, etc) über Plugins definieren üblicherweise eigene Arten von Zugangsdaten, um die Eingabe zu erleichtern.

Legacy-Konfiguration

In älteren Version von tenfold gab es keine Unterscheidung zwischen verschiedenen Arten von Zugangsdaten. Die Verbindungsart "Standard" entspricht den alten "typenlosen" Zugangsdaten. Es ist daher möglich, dass in Ihrer Konfiguration manche Plugins noch die Standard-Zugangsdaten verwenden, obwohl für dieses Plugin eigene Verbindungsarten vorhanden sind.

Folgende Plugins verwenden noch die Zugangsdatenart "Standard". Hier wird auch beschrieben, welche Bedeutung die Felder *Verbindung 1* und *Verbindung 2* für die jeweiligen Plugins haben.

Plugin	Verbindung 1	Verbindung 2
SSH Plugin	Hostname für die SSH Verbindung	Keine Bedeutung
Office 365 User Lifecycle Plugin	Keine Bedeutung	Keine Bedeutung
SAP User Lifecycle Plugin	Hostname des NetWeaver Servers	Keine Bedeutung

Hinweis zu Passworten

Die Passworte der Zugangsdaten werden in der tenfold Datenbank mit starker Verschlüsselung gespeichert und sind nicht - auch nicht per SQL Abfrage - einsehbar.

13.1.4 Active Directory

Die Zugangsdaten für die Verbindung zu Active Directory werden als einzige Ausnahme nicht über diese Funktion verwaltet. Stattdessen wird der Benutzername und das Passwort des administrativen Dienstkontos direkt in der Konfiguration der Domäne hinterlegt.

tenfold

Personen Ressourcen Berechtigungen Requests Organisation Workflows Provisioning Einstellungen

Domäne bearbeiten
Legen Sie die Einstellungen für die Domäne fest und konfigurieren Sie Ressourcen wie Fileserver oder Exchange Server

Speichern Verbindung testen Abbrechen

Allgemein Active Directory Fileserver Exchange SharePoint

Domäne

Name * tenfold.local UPN-Suffix tenfold.local

Interaktion ☒ Agent tenfold Server

Verbindungseinstellungen

Host localhost LDAP-Version 2

Authentifizierung Einfach LDAP-Port 389

Benutzername svc-tenfold@tenfold.local LDAPS-Port 636

Passwort Zertifikatsvalidierung ☐

..... SSL erzwingen ☒

Berechtigungen

Gruppen bearbeiten -

Gruppen löschen -

Mitglieder bearbeiten -

13.2 Feldmappings

13.2.1 Allgemeines

Feldmappings beziehen sich, so wie Feldregeln (siehe [Feldregeln](#)(see page 562)) auf die Personenfelder einer Person, also die Attribute die tenfold zu einer Person speichert. Die Personenfelder, die für eine Person verwaltet werden können, hängen von der Konfiguration der Personenfelder in der Personenart ab, welche der Person zugeordnet ist. Es ist somit möglich, unterschiedliche Feldkonfigurationen für unterschiedliche Personenarten zu konfigurieren. Zur Konfiguration der Personenfelder siehe auch [Personenarten](#)(see page 81). Die Aufgabe von Feldmappings ist es, die Personenfelder von tenfold auf Felder oder Attribute eines Fremdsystems zu übersetzen. Damit kann beispielsweise gesteuert werden, welche Attribute in Active Directory durch das Active Directory User Lifecycle Plugin mit welchen Inhalten aus Personenfeldern in tenfold befüllt werden sollen. Umgekehrt kann beispielsweise im Import Plugin konfiguriert werden, welche Spalte aus einer Importquelle in welches Personenfeld in tenfold übertragen werden soll.

13.2.2 Nutzung in Plugins

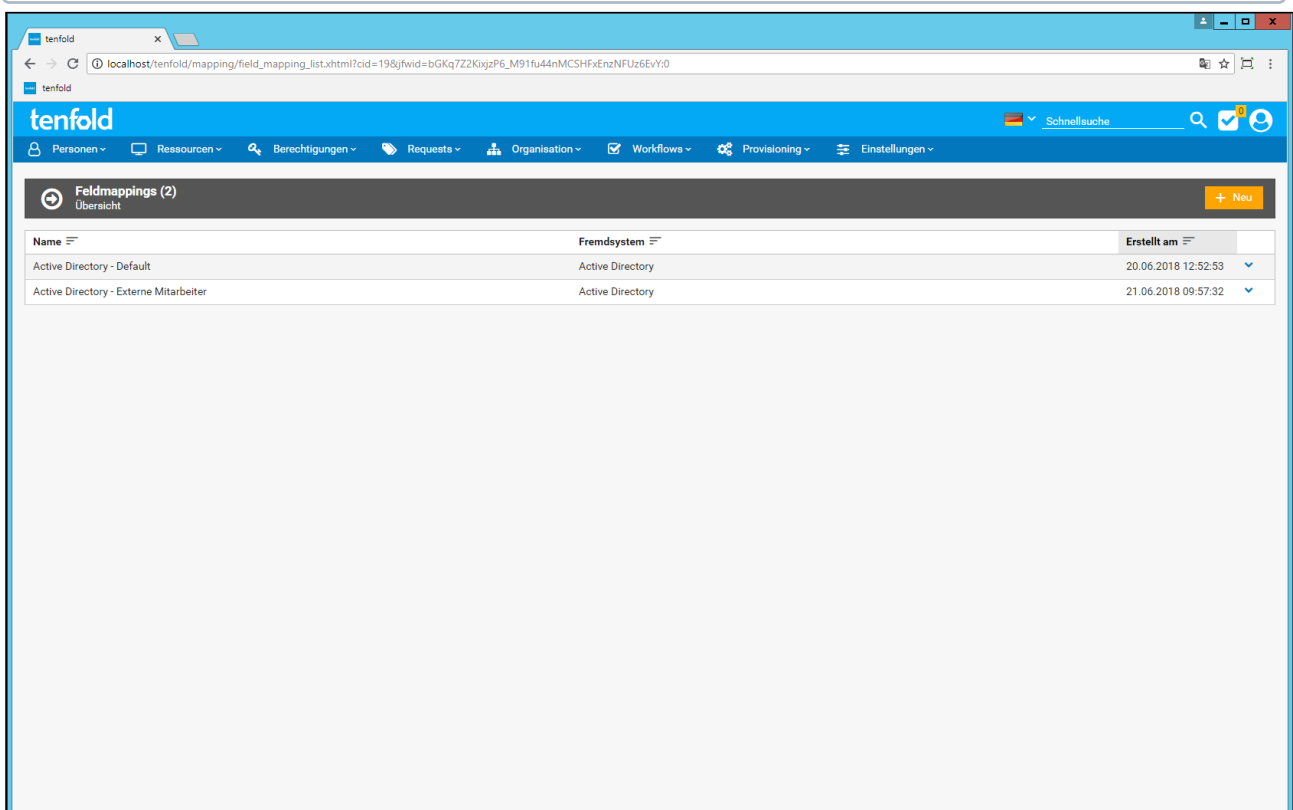
Ein Feldmapping bildet dabei die gesamte Konfiguration für ein Fremdsystem ab. Das bedeutet, dass alle Attribute beziehungsweise Personenfelder in dem jeweiligen Feldmapping enthalten sind. Das konfigurierte Feldmapping wird anschließend in der Konfiguration des gewünschten Plugins hinterlegt. Dadurch wird dem Plugin mitgeteilt, wie bei der Anlage oder Bearbeitung von Benutzerkonten hinsichtlich der zu setzenden Felder im Fremdsystem umgegangen werden soll. Plugins binden immer spezifische Systeme oder Anwendungen an tenfold an. Jedes System unterscheidet sich darin, welche Felder für Benutzerkonten überhaupt zur Verfügung stehen. Dadurch ist es erforderlich, dass im jeweiligen Feldmapping auf die von dem jeweiligen System unterstützten Felder referenziert wird. Außerdem müssen die im Fremdsystem verwendeten Bezeichnungen für die Felder verwendet werden, damit das Plugin anschließend weiß, welche

Felder im Fremdsystem zu adressieren sind. Damit im Feldmapping die richtigen Zielfelder zur Verfügung stehen, ist jedes Feldmapping einem spezifischen Fremdsystem zugeordnet. Die Auswahl der Fremdsysteme und die dementsprechend verfügbaren Attribute werden automatisch durch die Installation der jeweiligen Plugins bereitgestellt. So wird beispielsweise bei der Installation der Active Directory User Lifecycle Plugins automatisch ein Fremdsystemtyp "Active Directory" installiert, welcher die Standard-LDAP-Attribute des Active Directory beinhaltet.

13.2.3 Verwaltung

Benötigte Berechtigung

Für die Verwaltung der Feldmappings ist die Systemberechtigung "Manage Field Mappings" (8093) erforderlich.



Die Verwaltung der Feldmappings kann über Menü > Provisioning > Feldmappings erreicht werden. Die Maske listet dabei alle verfügbaren Feldmappings auf, welche im Kontextmenü angezeigt, bearbeitet, kopiert und gelöscht werden können.

13.2.4 Anlage und Bearbeitung

Sie können ein neues Feldmapping durch den Button "Neu" anlegen. Ein bestehendes Feldmapping kann durch Klick auf den Punkt "Bearbeiten" im Kontextmenü der jeweiligen Zeile bearbeitet werden.

Feldmappings
Hier können Sie ein Feldmapping bearbeiten

[Speichern](#) [Abbrechen](#)

Feldmapping

Name *

Beschreibung

Fremdsystem * Active Directory

Export von tenfold

[+ Hinzufügen](#)

Active Directory	tenfold
givenName	Vorname
sn	Nachname
department	Abteilung - Name

Import zu tenfold

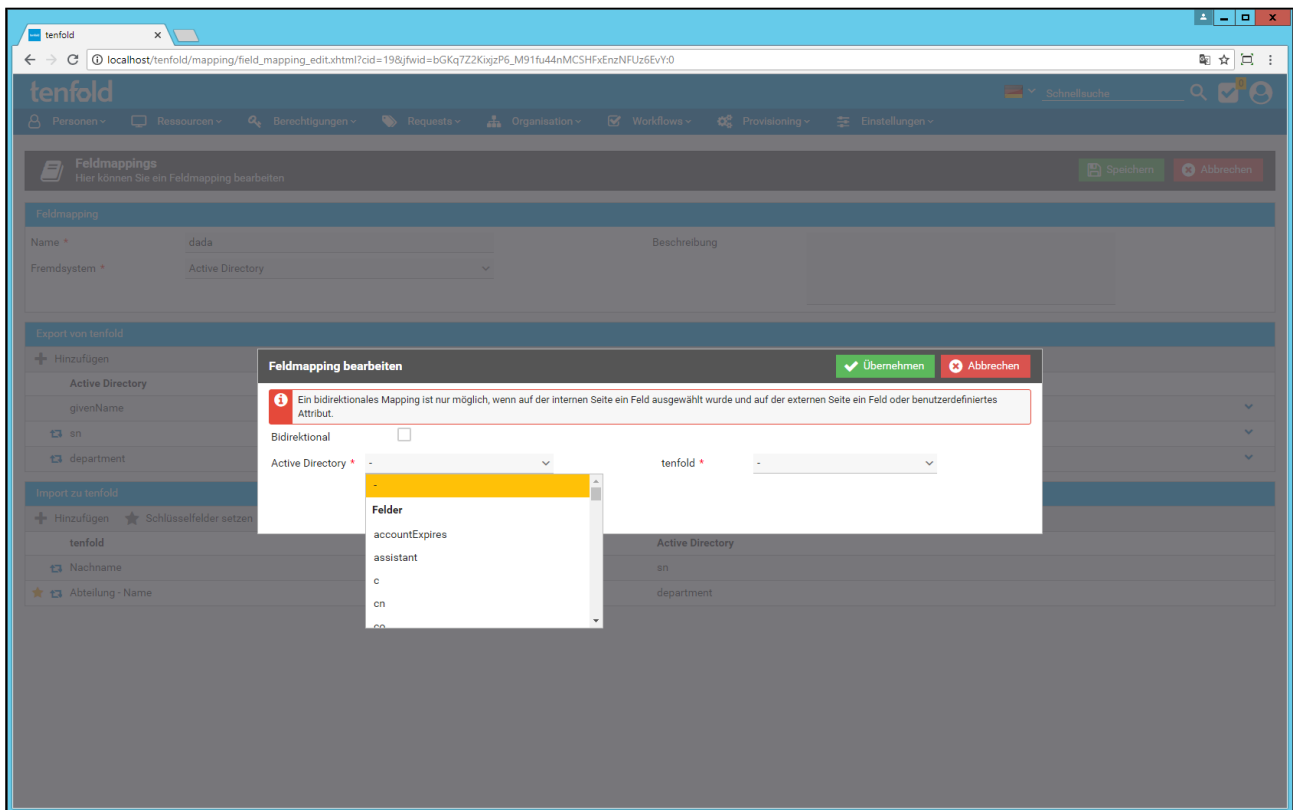
[+ Hinzufügen](#) [★ Schlüsselfelder setzen](#)

tenfold	Active Directory
Nachname	sn
Abteilung - Name	department

Im oberen Bereich kann dem Feldmapping ein Name gegeben werden, der zur Anzeige in tenfold genutzt wird. Zusätzlich kann eine Beschreibung hinterlegt werden. Anschließend muss für die Einstellung "Fremdsystem" das gewünschte System ausgewählt werden. Sobald ein System ausgewählt wurde, werden die verfügbaren Attribute oder Felder des gewählten Systems geladen und stehen für neue Einträge zur Verfügung.

Feld hinzufügen oder bearbeiten

Jeder Eintrag in der Tabelle "Export von tenfold" stellt das Mapping von einem Zielfeld im Fremdsystem und einem Quellfeld in tenfold dar. Dadurch wird definiert, wie das jeweilige Zielfeld im Fremdsystem durch tenfold gesetzt werden soll.



Über den Button "Hinzufügen" kann ein neuer Eintrag in der Liste erstellt werden. Ein Eintrag kann über das Kontextmenü und die Option "Bearbeiten" verändert und mit der Option "Löschen" aus der Tabelle entfernt werden.

Für den Eintrag muss nun auf der linken Seite das jeweilige Attribut des Fremdsystems, welches durch tenfold gesetzt werden soll, ausgewählt werden. Die verfügbare Auswahl hängt dabei vom zuvor gewählten Fremdsystem ab. Active Directory bietet beispielsweise über LDAP andere Attribute zur Verwaltung an, als dies SAP über das USER-BAPI macht.

Sobald auf der linken Seite das gewünschte Attribut oder Feld ausgewählt wurde, muss anschließend auf der rechten Seite ausgewählt werden, mit welchem Personenfeld aus tenfold das gewählte Attribut oder Feld im Fremdsystem gesetzt werden soll. Es stehen dabei mehrere Optionen zur Verfügung:

Einträge unter "Felder"

Bei den Einträgen unter Felder handelt es sich um die verfügbaren Personenfelder in tenfold. Für Objektwerte (bei denen das Personenfeld auf ein anderes Objekt in tenfold verweist, wie beispielsweise eine Abteilung) können auch auf die einzelnen Felder des Objekts zugegriffen werden. So ist es für Abteilungen beispielsweise möglich, sowohl auf den Namen, als auch auf den Kurznamen der Abteilung zu verweisen. Beispiel: Möchte man in das Attribut "department" im Active Directory den Kurznamen der Abteilung der jeweiligen Person eintragen, so wählt man auf der linken Seite "department" und auf der rechten Seite "Abteilung - Kurzname" aus.

Einträge unter "Snippets"

Die Einträge im Abschnitt "Snippets" stellen häufig benötigte Zusammensetzungen mehrerer Personenfelder in tenfold zur Verfügung.

Beispiel: Möchte man das Attribut "displayName" im Active Directory mit dem Nachnamen, einem Komma und dem Vornamen der Person befüllen, so wählt man das Snippet "[LastName], [FirstName]" aus.

Benutzerdefiniertes Snippet

Im Abschnitt "Snippet" gibt es darüber hinaus die Einstellungsmöglichkeit "Benutzerdefiniertes Snippet". Sobald man diese Option wählt, erscheint ein Eingabefeld "Snippet". In diesem kann über Script ein benutzerdefinierter Rückgabewert generiert werden. Über die Variable "person" haben Sie Zugriff auf die Personenfelder.

Wert

Über die Einstellung "Wert" ist es möglich, ein Attribut im Zielsystem immer mit einer fixen Zeichenkette zu setzen. Sobald die Einstellung gewählt wurde, kann im Feld "Wert" die gewünschte Zeichenkette eingegeben werden.

Feld entfernen

Ein bestehendes Feld kann über das Kontextmenü und die Option "Löschen" wieder aus dem Mapping entfernt werden.

Import und bidirektionale Verarbeitung

Abhängig vom ausgewählten Fremdsystem gibt es die Möglichkeit, Felder aus dem Fremdsystem nach tenfold zu übertragen. Besondere Bedeutung hat dies im Rahmen des Import Plugin, bei welchem aus einem Quellsystem Personendaten nach tenfold übertragen werden. Die Vorgehensweise ist dabei grundsätzlich die gleiche, wie beim Export von Daten aus tenfold in ein Fremdsystem. Lediglich die Anordnung ist dabei vertauscht: auf der linken Seite befindet sich das tenfold Personenfeld, welches gesetzt werden soll, und auf der rechten Seite befindet sich das Attribut oder Feld aus dem Fremdsystem, welches als Quelle für die Daten dient.

Wenn dies vom Fremdsystem unterstützt wird, ist es darüber hinaus auch möglich, ein Feldmapping bidirektional einzurichten. Das bedeutet, dass tenfold beim Anlegen oder Bearbeiten von Benutzerkonten die ausgewählten Felder beschreibt, aber gleichzeitig im Rahmen der Synchronisation mit dem betreffenden System die Inhalte der gemappten Felder prüft und etwaige Änderungen, die im Fremdsystem stattgefunden haben, nach tenfold zurück synchronisiert. Diese Änderungen werden in Form von entsprechenden Requests dokumentiert, wobei die Details von der Handhabung des jeweiligen Plugins abhängen.

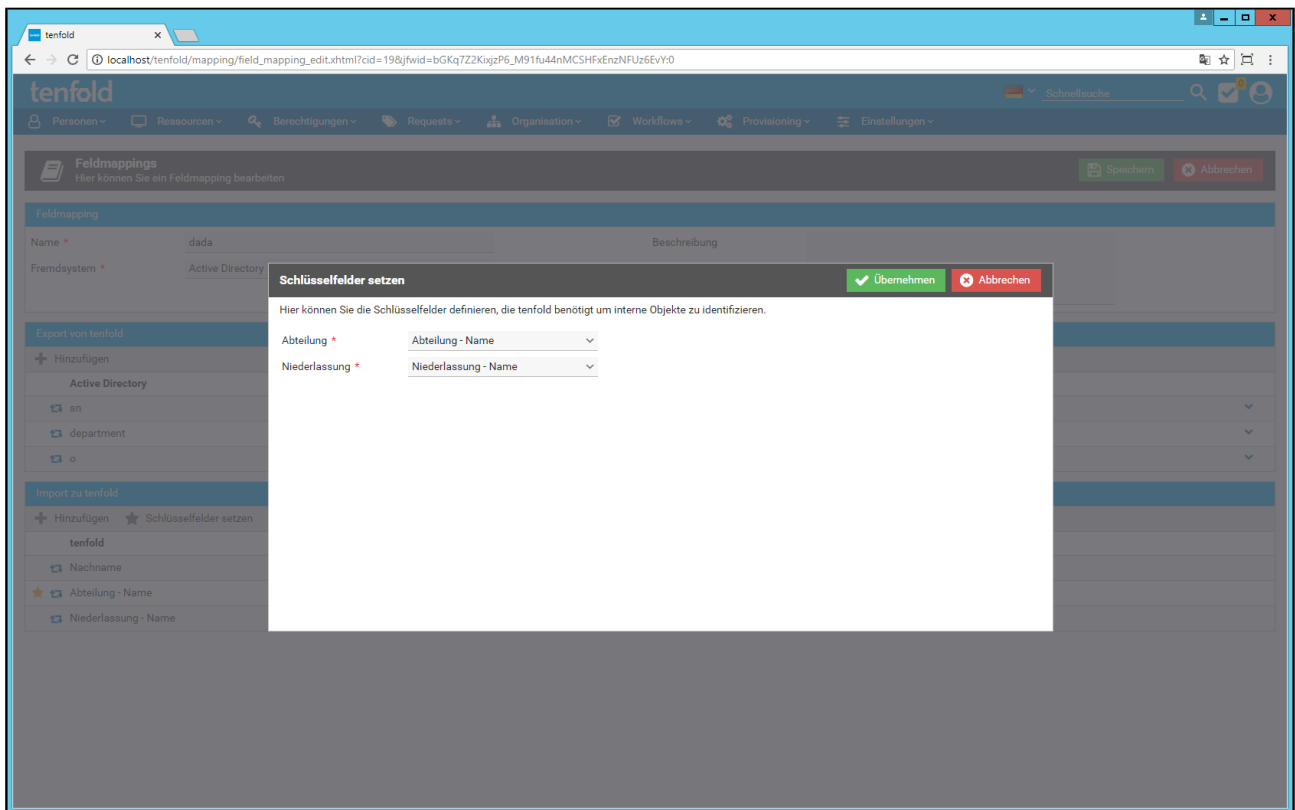
Wenn ein Feld zur bidirektionalen Verarbeitung vorgesehen wird, so wird automatisch ein Eintrag in der Tabelle "Import zu tenfold" angelegt.

Hinweis

Aktuell wird die bidirektionale Verarbeitung nur vom Active Directory User Lifecycle Plugin unterstützt.

Schlüsselfelder

Die Konfiguration von Schlüsselfeldern ist notwendig, wenn aus einem Fremdsystem Daten nach tenfold importiert werden sollen. Beim Export von Personenfeldern in ein Fremdsystem ist diese Einstellung nicht erforderlich. Der Button "Schlüsselfelder setzen" ist deshalb nur aktiv, wenn das ausgewählte Fremdsystem den Import von Daten erlaubt und damit die Tabelle "Import nach tenfold" sichtbar ist.

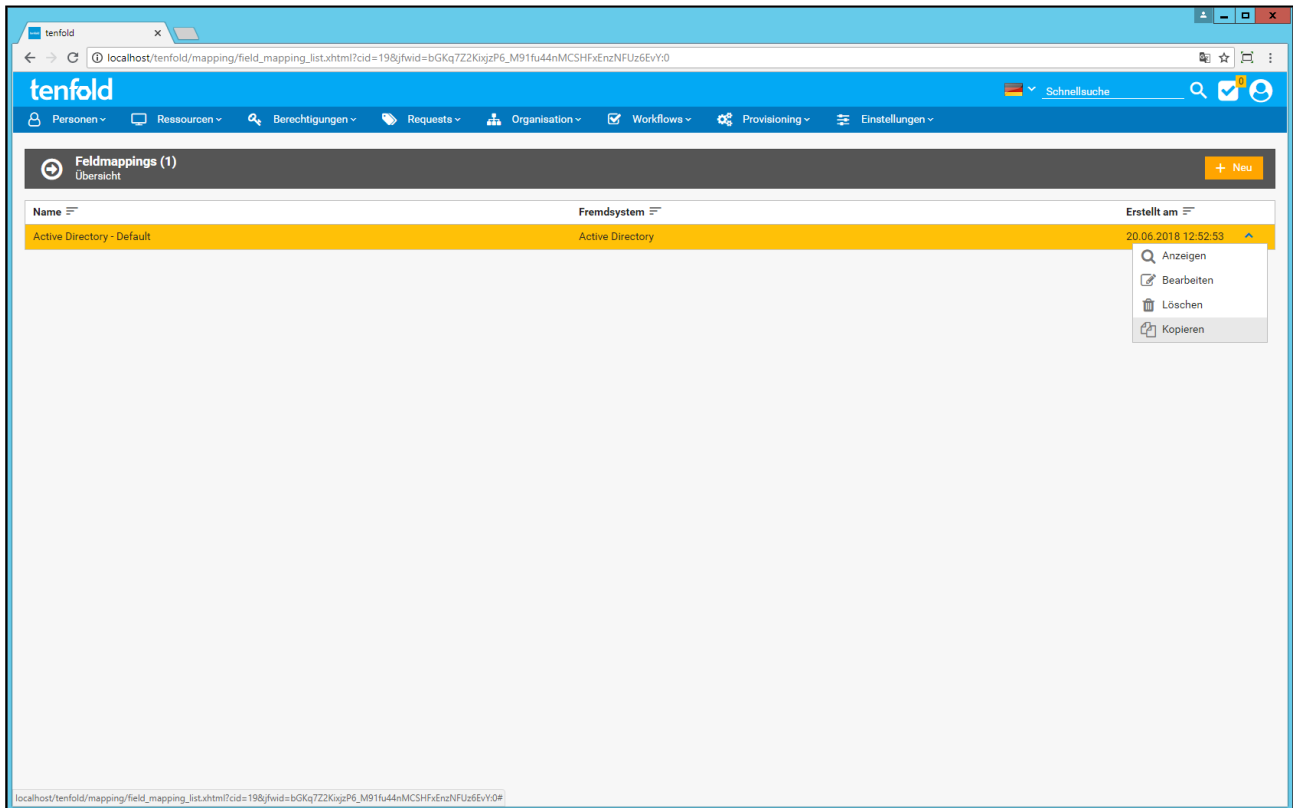


Ein Schlüsselfeld muss hinterlegt werden, um Daten aus einem Fremdsystem (welche - mit wenigen Ausnahmen - grundsätzlich immer als Zeichenketten behandelt werden) auf Objektwerte in tenfold umzuschlüsseln. Beispielsweise ist die Definition eines Schlüsselfeldes erforderlich, wenn das Attribut "department" im Active Directory (eine freie Zeichenkette) auf eine bestimmte Abteilung in tenfold umgeschlüsselt werden soll. Das Schlüsselfeld bestimmt dabei, mit welchem Feld eines Objektwerts die Zeichenkette aus dem Fremdsystem verglichen wird, um Gleichheit festzustellen. So kann bei Abteilungen beispielsweise festgelegt werden, dass Attribut "department" mit dem Kurznamen der Abteilung verglichen wird, um festzustellen, welche Abteilung bei der betroffenen Person ausgewählt werden soll.

Nachträgliche Änderungen

Es gilt zu beachten, dass jegliche Änderungen, die an einem Feldmapping durchgeführt werden nur für alle zukünftigen Änderungen und Synchronisationen gelten. Wird das Feldmapping verändert, werden nicht automatisch alle Benutzerkonten der betroffenen Personen auf Basis des neuen Feldmappings aktualisiert.

13.2.5 Kopieren



Ein bestehendes Feldmapping kann kopiert werden, um ausgehend von der existierenden Konfiguration ein neues Feldmapping zu erzeugen. Finden Sie in der Liste aller Feldmapping den Eintrag, der kopiert werden soll und wählen Sie die Option "Kopieren" aus dem Kontextmenü. Anschließend wird dieses Feldmapping temporär kopiert und Sie haben die Möglichkeit die Einstellungen anzupassen. Das Feldmapping wird erst dann tatsächlich in der Datenbank gespeichert, wenn Sie nach dem Durchführen der Anpassungen den Button "Speichern" klicken.

13.2.6 Löschen

Ein bestehendes Feldmapping kann über die Option "Löschen" im Kontextmenü der jeweiligen Zeile gelöscht werden.

13.2.7 Weiterführende Hinweise

Für jedes Fremdsystem (und damit gegebenenfalls für jedes Plugin) existieren hinsichtlich der Felder oder Attribute unter Umständen spezielle Einstellungen oder Optionen. Die Dokumentation hierfür ist bei den jeweiligen Plugins zu finden.

13.3 Feldregeln

13.3.1 Allgemein

Feldregeln sind ein zentrales Werkzeug in tenfold, um Verhaltensweisen des Systems von den Feldinhalten einer Person abhängig zu machen. Sie werden an mehreren Punkten genutzt, zum Beispiel:

- Für die automatische Zuordnung von Profilen (siehe auch [Profile](#)(see page 168))

- Für Einstellungen in Plugins, zum Beispiel, um zu steuern, in welcher Active Directory-OU sich ein Benutzerkonto befinden soll (siehe auch [Active Directory User Lifecycle](#)(see page 665))

Eine Feldregel besteht immer aus einer oder mehreren Bedingungen. Diese Bedingungen beziehen sich auf zu definierende Feldinhalte. Beispiele hierfür können sein:

- Die Abteilung muss "Finanzen" sein
- Die Stadt der primären Niederlassung muss mit "W" beginnen
- Die Personenart darf nicht "Mitarbeiter" sein

Innerhalb einer Feldregel kann es mehrere solcher Bedingungen geben. Diese sind immer mit "und" verknüpft. Das bedeutet, dass, wenn mehrere Bedingungen in einer Regel definiert sind, alle Bedingungen zutreffen müssen. Treffen nicht alle Bedingungen zu, so trifft die Regel als ganzes nicht zu.

13.3.2 Verwaltung von Feldregeln

Benötigte Berechtigung

Für die Verwaltung der Feldregeln muss entweder die Berechtigung "Manage Ressources" (8050) oder "Profiles" (8070) zugeordnet sein.

Feldregeln können über den Menüpunkt *Provisioning > Regelwerke > Feldregeln* zentral verwaltet werden.

Name	Regel
Abteilung IT	Abteilung ist IT (exakt)
AUTO: COMPANY=tenfold	Unternehmen ist tenfold (exakt) (nur Hauptniederlassung)
AUTO: COMPANY=tenfold	Unternehmen ist tenfold (exakt) (nur Hauptniederlassung)
AUTO: COMPANY=tenfold	Unternehmen ist tenfold (exakt) (nur Hauptniederlassung)
AUTO: COMPANY=tenfold	Unternehmen ist tenfold (exakt) (nur Hauptniederlassung)
AUTO: COMPANY=tenfold	Unternehmen ist tenfold (exakt) (nur Hauptniederlassung)
AUTO: COUNTRY=Austria	Niederlassungsstaat ist Austria (alle)
AUTO: COUNTRY=Austria	Niederlassungsstaat ist Austria (alle)
AUTO: COUNTRY=Austria	Niederlassungsstaat ist Austria (alle)
AUTO: COUNTRY=Austria	Niederlassungsstaat ist Austria (alle)
AUTO: COUNTRY=Austria	Niederlassungsstaat ist Austria (alle)
AUTO: DEP=IT	Abteilung ist IT (exakt)
AUTO: DEP=IT	Abteilung ist IT (exakt)
AUTO: DEP=IT	Abteilung ist IT (exakt)
AUTO: DEP=IT	Abteilung ist IT (exakt)
AUTO: DEP=IT	Abteilung ist IT (exakt)
AUTO: DEP=IT POS=Meine Testposition	Abteilung ist IT (exakt) und Position ist Meine Testposition
AUTO: DEP=IT POS=Meine Testposition	Abteilung ist IT (exakt) und Position ist Meine Testposition
AUTO: DEP=IT POS=Meine Testposition	Abteilung ist IT (exakt) und Position ist Meine Testposition
AUTO: DEP=IT POS=Meine Testposition	Abteilung ist IT (exakt) und Position ist Meine Testposition
AUTO: DEP=IT POS=Meine Testposition	Abteilung ist IT (exakt) und Position ist Meine Testposition

Die Maske zeigt eine Liste aller hinterlegten Feldregeln an. Über den Button "Neu" kann eine neue Regel hinterlegt werden. Über das Kontextmenü der jeweiligen Zeile kann eine Regel angezeigt, bearbeitet oder gelöscht werden.

Feldregeln können nur dann gelöscht werden, wenn sie nicht mehr verwendet werden. Ist die Feldregel noch in einer Einstellung hinterlegt (dies gilt auch für alle Einstellungen in Plugins), kann sie nicht gelöscht werden.

13.3.3 Anlage und Bearbeitung

Kopfdaten

The screenshot shows the 'Neue Feldregel' (New Field Rule) form in the tenfold web interface. The form is divided into three main sections:

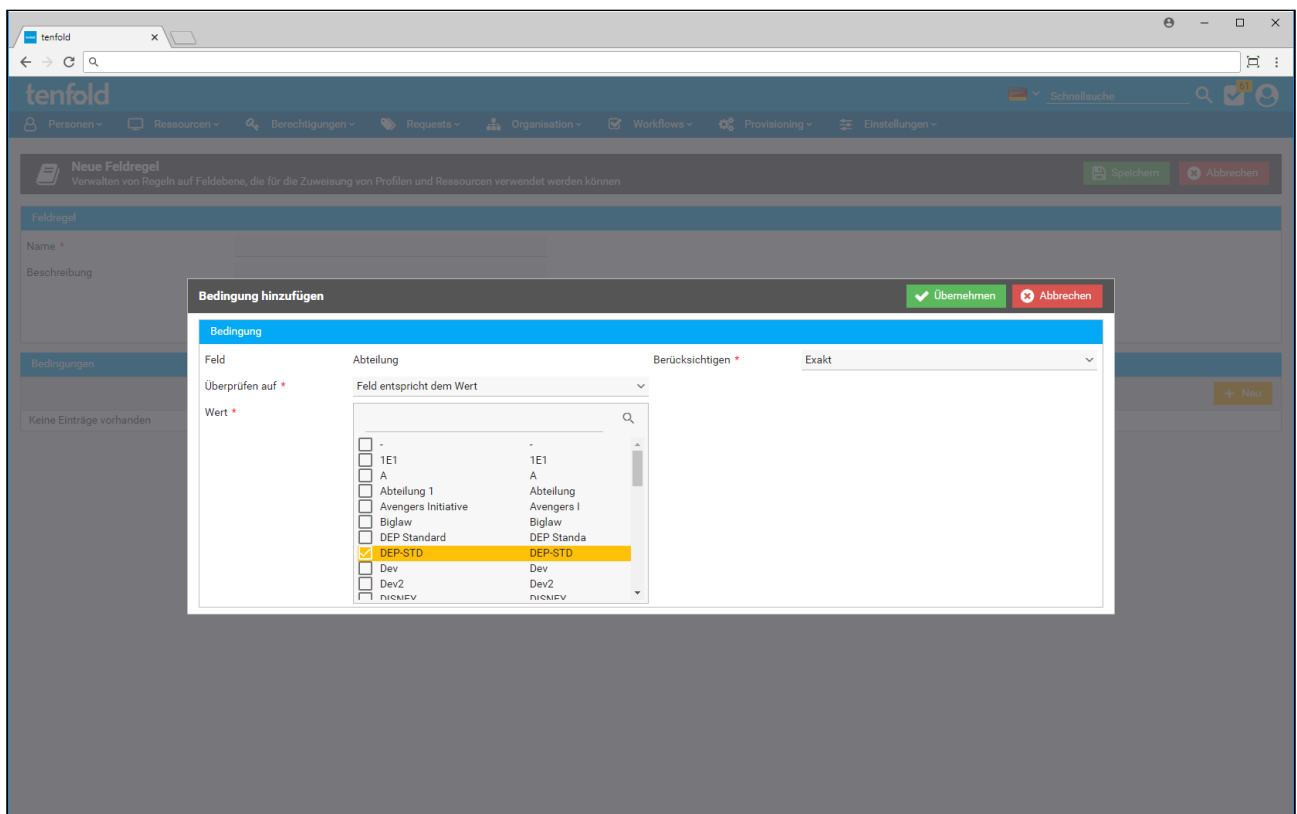
- Feldregel**: This section contains two input fields: 'Name' (with a red asterisk indicating it is required) and 'Beschreibung'.
- Bedingungen**: This section contains a '+ Neu' button to add new conditions.
- Keine Einträge vorhanden**: This section indicates that there are no entries currently present.

Eine Feldregel besteht aus drei Einstellungen, die bei der Anlage einer neuen Regel oder der Bearbeitung einer bestehenden Regel gesetzt werden können:

- Name - die Bezeichnung, die auf der tenfold-Oberfläche verwendet wird.
- Beschreibung - es kann eine Beschreibung hinterlegt werden, wo beispielsweise auf Zweck oder Nutzung der Regel eingegangen wird.
- Bedingungen - es handelt sich hierbei um eine Tabelle von Bedingungen, die erfüllt werden müssen, damit die Regel als Ganzes erfüllt wird.

Bedingungen

Um eine neue Bedingung hinzuzufügen, drücken Sie den Button "Neu" im Abschnitt "Bedingungen".



Innerhalb einer Bedingung hängen die Einstellungsmöglichkeiten davon ab, auf welches Personenfeld geprüft werden soll. Die folgenden Abschnitte beschreiben die Möglichkeiten.

Prüfung auf Objektwert

The screenshot shows the tenfold web interface. At the top, there's a navigation bar with various icons and a search bar. Below it, a header section contains the text 'Neue Feldregel' and 'Verwalten von Regeln auf Feldebene, die für die Zuweisung von Profilen und Ressourcen verwendet werden können'. The main content area is divided into sections: 'Feldregel' with fields for 'Name' and 'Beschreibung', and 'Bedingungen' which currently shows 'Keine Einträge vorhanden'. A modal dialog titled 'Bedingung hinzufügen' is open, featuring a 'Feld' dropdown set to 'Überprüfen auf' and a 'Wert' dropdown set to 'Feld entspricht dem Wert'. Below the 'Wert' dropdown, a list of values is shown: 'Mitarbeiter' (checked) and 'Testbenutzer' (unchecked). The dialog includes 'Übernehmen' and 'Abbrechen' buttons.

Die einfachste Form der Prüfung ist der Vergleich mit einem Objektwert. Diese Prüfung steht für alle Personenfelder zur Verfügung, welche auf ein anderes Objekt in tenfold referenzieren (zum Beispiel auf eine Abteilung oder eine Personenart). Es kann geprüft werden:

- ob das Personenfeld einem der ausgewählten Werte entspricht (Feld entspricht dem Wert)
- ob das Personenfeld nicht einem der ausgewählten Werte entspricht (Feld entspricht nicht dem Wert)
- ob das Personenfeld überhaupt einen Wert hat oder nicht (Feld ist leer / Feld ist nicht leer)

Anschließend können die gewünschten Werte selektiert werden. Die Prüfung der Werte erfolgt hierbei auf Basis von "oder". Es muss also einer der Werte auf die jeweilige Prüfung zutreffen, nicht alle Werte (eine Prüfung auf alle Werte würde immer fehlschlagen, da in den meisten Fällen nur ein Wert in einem Personenfeld hinterlegt werden kann).

Prüfung auf Textfeld

Diese Prüfung steht für alle Personenfelder zur Verfügung, welche die Möglichkeit einer freien Texteingabe ermöglichen. Zusätzlich zu den Bedingungen, die auch für die Prüfung auf Objektwerte gelten, kann für Textfelder eine zusätzliche Einschränkung erfolgen. So kann geprüft werden, ob die Zeichenkette des Feldinhalts:

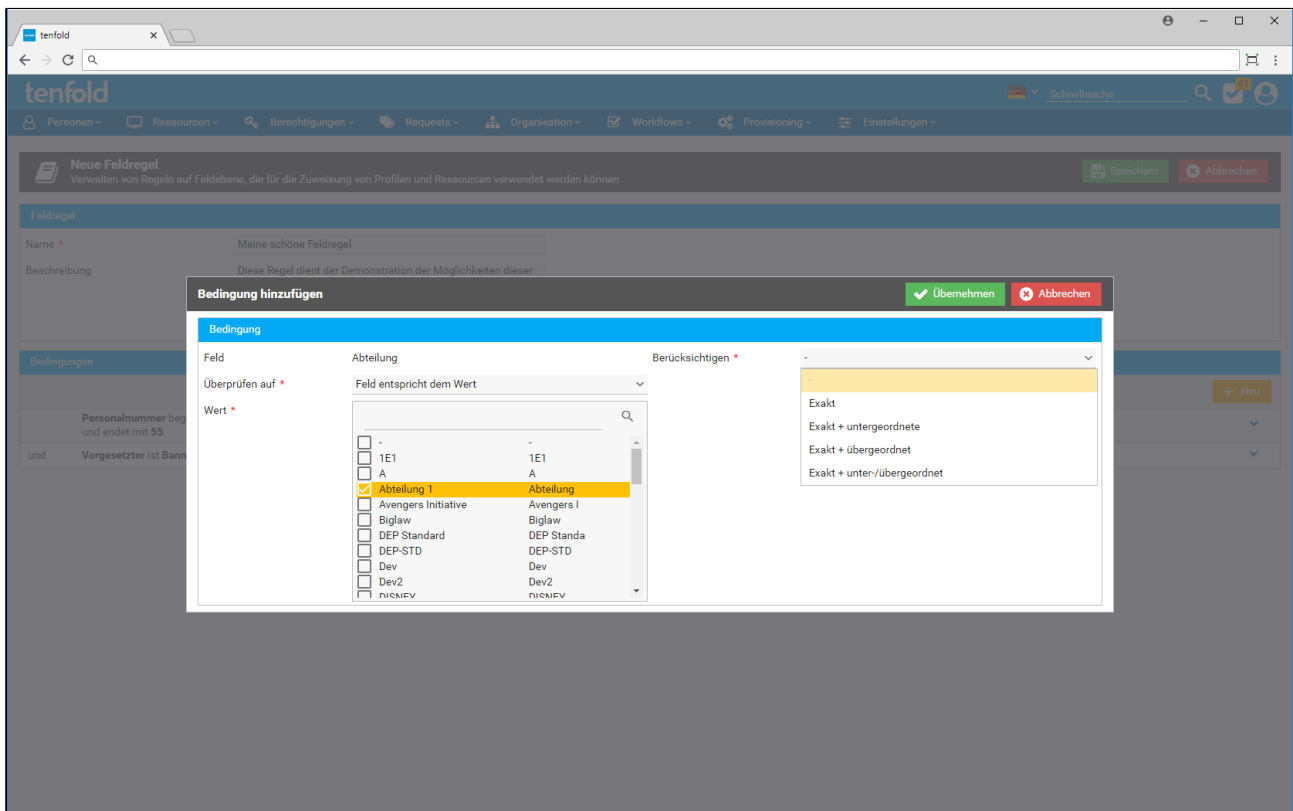
- mit einer bestimmten Zeichenkette beginnt ("Beginnt mit")
 - Beispiel: "ABCD" beginnt mit "A" und mit "AB"
- mit einer bestimmten Zeichenkette endet ("Endet mit")
 - Beispiel: "ABCD" endet mit "D"
- eine bestimmte Zeichenkette enthält ("Enthält")
 - Beispiel: "ABCD" enthält "BCD"
- genau einer bestimmten Zeichenkette gleicht ("Ist gleich")
 - Beispiel: "ABCD" ist gleich mit "ABCD"

Hinweis zu Groß- und Kleinschreibung

Bei Textprüfungen wird auf Groß- und Kleinschreibung geachtet. "ABCD" ist somit nicht gleich zu "Abcd".

Diese Konditionen können über den Button "Weitere Überprüfung hinzufügen" mit anderen Konditionen verknüpft werden. So kann beispielsweise überprüft werden, ob eine Zeichenkette mit einer bestimmten Zeichenfolge beginnt und mit einer anderen bestimmten Zeichenfolge endet. Die Konditionen untereinander sind immer mit "und" verknüpft. Es müssen somit alle Konditionen erfüllt werden, damit die Bedingung als Ganzes erfüllt wird.

Prüfung auf hierarchische Objektwerte



Ein spezieller Fall der Prüfung auf Objektwerte ist die Prüfung auf Objekte, welche in tenfold hierarchisch organisiert werden können. Dies sind:

- Abteilungen
- Unternehmen

Beide dieser Objekte können für jeden Eintrag einen übergeordneten Eintrag haben, um Hauptabteilungen und Unterabteilungen oder Konzernbeteiligungen abzubilden.

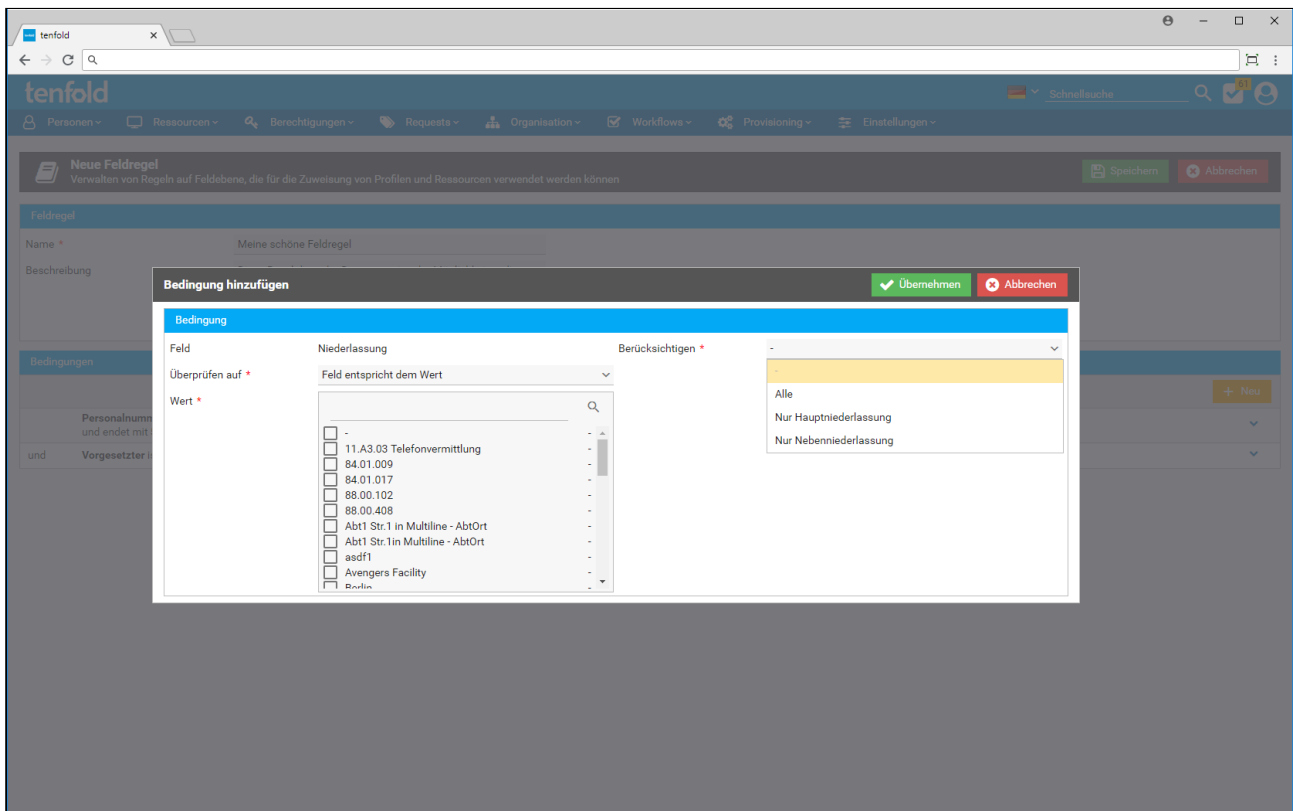
Bei der Prüfung kann nach der Auswahl des gewünschten Eintrags nunmehr bestimmt werden, welche Einträge - in Bezug auf die Hierarchie - berücksichtigt werden sollen:

- Exakt: Die Bedingung gilt nur als erfüllt, wenn der Feldinhalt exakt den ausgewählte(n) Abteilung(en) oder Unternehmen entspricht
- Exakt und untergeordnete: Die Bedingung gilt zusätzlich als erfüllt, wenn der Feldinhalt eine Abteilung oder einem Unternehmen entspricht, welches der Auswahl untergeordnet ist
- Exakt und übergeordnete: Die Bedingung gilt zusätzlich als erfüllt, wenn der Feldinhalt eine Abteilung oder einem Unternehmen entspricht, welches der Auswahl übergeordnet ist
- Exakt und unter-/übergeordnet: Diese Einstellung verbindet die beiden vorgenannten Einstellungen

Prüfung auf Unternehmen

Das Objekt "Unternehmen" steht nicht als selbstständiges Personenfeld zur Verfügung. Wenn auf das Objekt "Unternehmen" geprüft wird, erfolgt die Prüfung immer auf das Unternehmen der oder des zugeordneten Niederlassung(en).

Prüfung auf Niederlassungen



Einen zusätzlichen Spezialfall bildet die Prüfung auf Niederlassungen ab. Das Personenfeld "Niederlassung" kann einen einzelnen Wert beinhalten, aber es kann auch mehrere Werte beinhalten, wenn für die jeweilige Personenart die Einstellung "Mehrere Niederlassungen" aktiviert ist (siehe dazu auch [Personenarten](#)(see page 81)). Wenn einer Person mehrere Niederlassungen zugeordnet sind, so muss eine der zugeordneten Niederlassungen als "Hauptniederlassung" gekennzeichnet sein. Entsprechend dieser Unterscheidung lässt sich bei der Prüfung auf das Personenfeld "Niederlassung" folgende Einstellung treffen:

- Alle: Es werden alle zugeordneten Niederlassungen mit den ausgewählten Niederlassungen in der Bedingung verglichen. Trifft eine davon zu, gilt die Bedingung als erfüllt.
- Nur Hauptniederlassung: Die Bedingung gilt nur als erfüllt, wenn die als Hauptniederlassung gekennzeichnete Niederlassung der Auswahl entspricht.
- Nur Nebenniederlassung: Die Bedingung gilt nur als erfüllt, wenn eine der nicht als Hauptniederlassung gekennzeichneten Niederlassungen der Auswahl entspricht.

Prüfung auf Personenlisten

Mit dem Bedingungsmodus "Personenliste" kann, statt der Prüfung auf den Inhalt eines Personenfeldes, geprüft werden, ob die Person Mitglied einer bestimmten Personenliste (siehe [Personenlisten](#)(see page 116)) ist. Alternativ kann geprüft werden, ob die Person *nicht* Mitglied einer bestimmten Liste ist.

Um eine Bedingung zur Prüfung auf Mitgliedschaft einer Personenliste zu konfigurieren, wählen Sie als Bedingungsmodus "Personenliste" aus. Im Feld "Überprüfen auf" wählen Sie aus, ob Sie prüfen möchten, ob die Person Mitglied der ausgewählten Personenlisten sein soll oder, ob die Person nicht Mitglied der Listen sein darf.

In der Einstellung "Personenlisten" wählen Sie nun die Personenlisten aus, auf welche geprüft werden soll.

Auswählbare Personenlisten

Für Bedingungen von Feldregeln können nur Listen vom Typ "Personenauswahl" ausgewählt werden.

Auswahl mehrere Personenlisten

Wenn Sie mehrere Personenlisten auswählen, muss die Person auf zumindest einer der Listen aufscheinen, wenn die Auswahl "Ist Mitglied" getroffen wurde. Mit der Einstellung "Ist nicht Mitglied" darf die Person in keiner der ausgewählten Listen Mitglied sein.

Prüfung auf Datumsfelder

Für alle in tenfold vorhandenen Datumsfelder kann geprüft werden, ob ein Wert vorhanden ist oder nicht.

Zeiträume

Eine Prüfung auf bestimmte Zeiträume ist nicht möglich.

Zusammenfassung

The screenshot shows the 'Feldregel bearbeiten' (Edit Field Rule) page in the tenfold application. The page has a blue header with the tenfold logo and navigation links: Personen, Ressourcen, Berechtigungen, Requests, Organisation, Workflows, Provisioning, and Einstellungen. A search bar and a 'Schnellauche' button are also present.

The main content area is titled 'Feldregel bearbeiten' and includes a subtitle 'Verwalten von Regeln auf Feldebene, die für die Zuweisung von Profilen und Ressourcen verwendet werden können'. There are two buttons: 'Speichern' (Save) and 'Abbrechen' (Cancel).

The form consists of two main sections: 'Feldregel' (Field Rule) and 'Bedingungen' (Conditions).

Feldregel Section:

- Name:** Meine schöne Feldregel
- Beschreibung:** Diese Regel dient der Demonstration der Möglichkeiten dieser Funktion.

Bedingungen Section:

- Condition 1:** Personalnummer beginnt mit 10 und endet mit 55
- Condition 2:** Vorgesetzter ist Banner Bruce (bruce.banner), Beckenbauer Susanne (sbeckenb) oder Berg Annett (aberg)

There is a '+ Neu' (New) button to add more conditions.

Zur vereinfachten Darstellung werden nach dem Speichern einer Bedingung alle Bedingungen in Textform dargestellt, um die manuelle Kontrolle der Regel zu vereinfachen.

Bearbeiten und Löschen

The screenshot shows the 'Feldregel bearbeiten' (Edit Field Rule) page in the tenfold application. The page has a blue header with the tenfold logo and navigation links: Personen, Ressourcen, Berechtigungen, Requests, Organisation, Workflows, Provisioning, and Einstellungen. A search bar and a language selector (Deutsch) are also present.

The main content area is titled 'Feldregel bearbeiten' and includes a subtitle: 'Verwalten von Regeln auf Feldebene, die für die Zuweisung von Profilen und Ressourcen verwendet werden können'. There are two buttons: 'Speichern' (Save) and 'Abbrechen' (Cancel).

The form is divided into two sections: 'Feldregel' and 'Bedingungen'.

Feldregel

Name *	Meine schöne Feldregel
Beschreibung	Diese Regel dient der Demonstration der Möglichkeiten dieser Funktion.

Bedingungen

Personalnummer beginnt mit 10 und endet mit 55

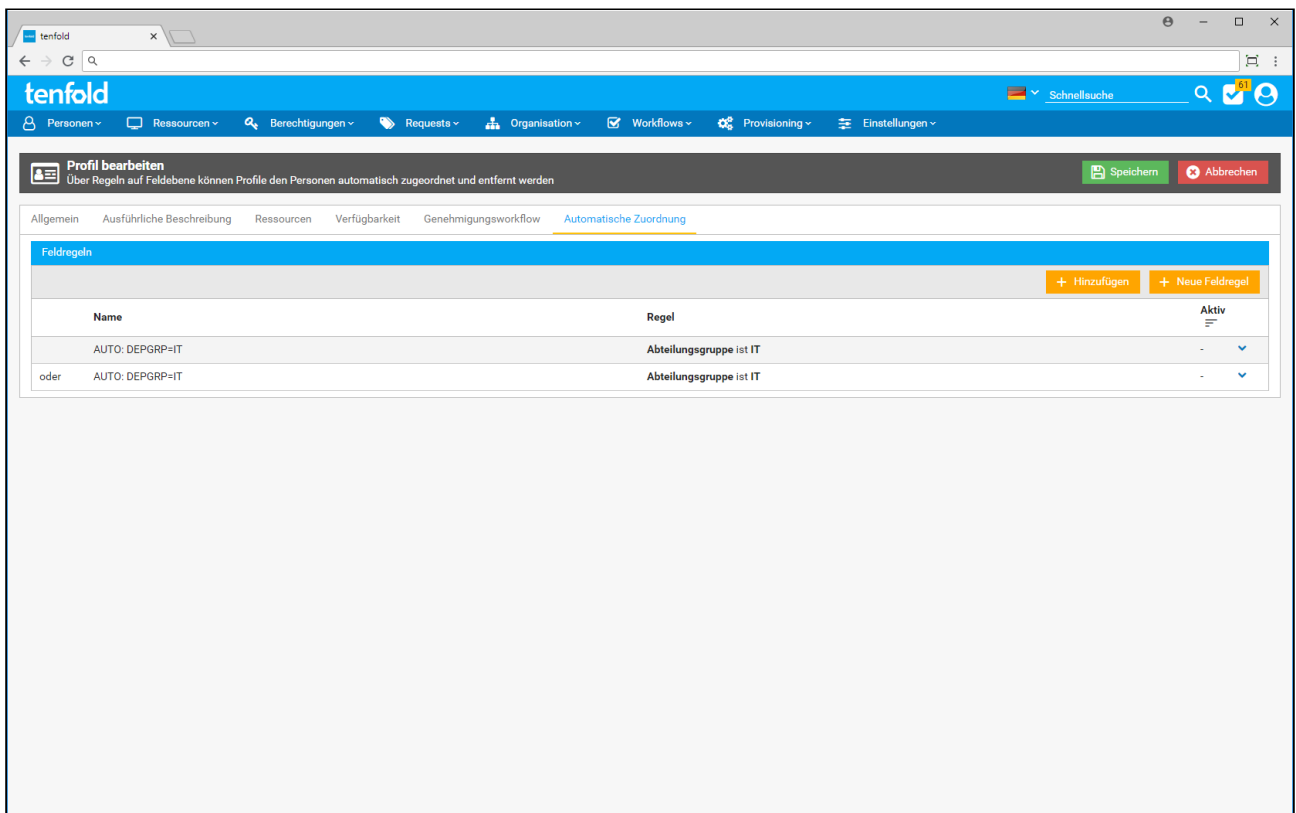
und Vorgesetzter ist Banner Bruce (bruce.banner), Beckenbauer Susanne (sbeckenb) oder Berg Annett (aberg)

A context menu is open over the first condition, showing the following options:

- Bearbeiten
- Löschen

Über das Kontextmenü der jeweiligen Bedingung kann eine einzelne Bedingung aus einer Feldregel entfernt werden oder deren Inhalt bearbeitet werden.

13.3.4 Vereinfachte Anlage



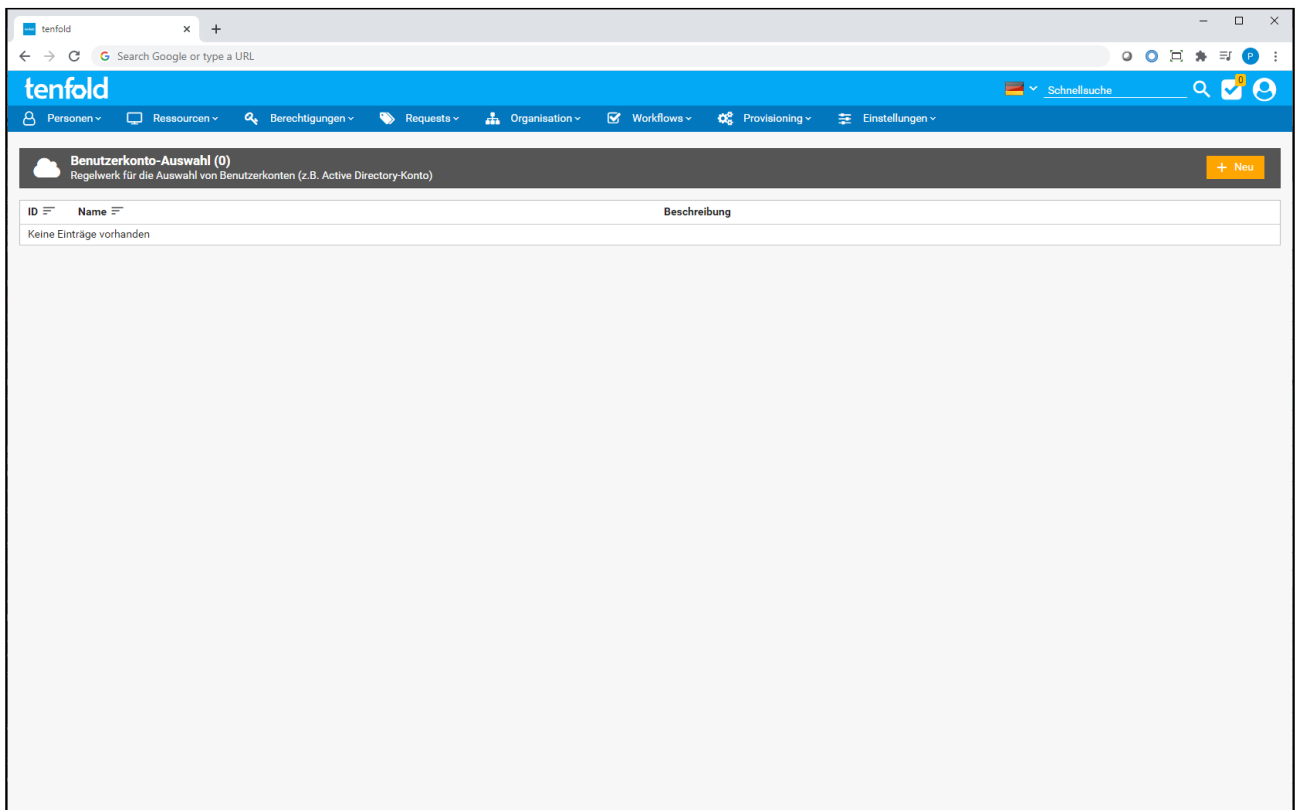
An vielen Stellen, an denen Feldregeln zum Einsatz kommen können, gibt es die Möglichkeit, über den Button "Neue Feldregel", direkt eine neue Feldregel anzulegen, ohne die aktuelle Maske verlassen zu müssen und in die Verwaltung für Feldregeln wechseln zu müssen.

13.3.5 Duplikate

Achtung

Bei der Anlage einer Feldregel erfolgt keine Prüfung dahingehend, ob es eventuell bereits eine bestehende Feldregel gibt, welche exakt die gleichen Bedingungen prüft. Es ist daher empfehlenswert gegebenenfalls, bevor eine neue Regel angelegt wird, zu überprüfen, ob die gewünschte Regel bereits im System existiert. Dadurch können unnötige Duplikate vermieden werden.

13.4 Benutzerkonto-Auswahl



Sie erreichen diese Maske im Menü unter Provisioning > Regelwerke > Benutzerkonto-Auswahl.

Benötigte Berechtigung

Für den Zugriff auf diese Maske wird die tenfold-Berechtigung "User Account Selection Rules administration" (8700) benötigt.

Auf dieser Maske lassen sich Regelwerke definieren, welche von Profilen benutzt werden können, um zu entscheiden, welchen Benutzerkonten Gruppen aus dem Profil zugeordnet werden, sollte eine Person mehrere Benutzerkonten haben. Näheres finden Sie unter [Profile](#) (see page 168). Wenn Sie einer Person mit mehreren Microsoft 365-Konten eine Gruppe zuordnen, so werden Sie gefragt welchem Konto die Gruppe hinzugefügt werden soll. Wenn Sie einem Profil eine Gruppe zuordnen, so können Sie im Vorfeld nicht wissen welche Konten eine Person, welcher das Profil einmal zugeordnet wird, haben wird. Daher ist es notwendig Regeln zu erstellen, welche Konten, in diesem Fall, die Gruppenmitgliedschaft erhalten.

13.4.1 Neue Regel erstellen

Klicken Sie in der Listenansicht auf die Schaltfläche *Neu*, um eine neue Regel anzulegen. Sie gelangen daraufhin auf folgende Maske:

tenfold | Schnellsuche

Personen | Ressourcen | Berechtigungen | Requests | Organisation | Workflows | Provisioning | Einstellungen

Neue Benutzerkonto-Auswahl
Regelwerk für die Auswahl von Benutzerkonten (z.B. Active Directory-Konto)

[Speichern](#) [Abbrechen](#)

Allgemein

Name * Kontotyp *

Beschreibung Ergebnis der Auswertung *

Bedingungen

Sie können die Reihenfolge mittels Drag-and-drop verändern.

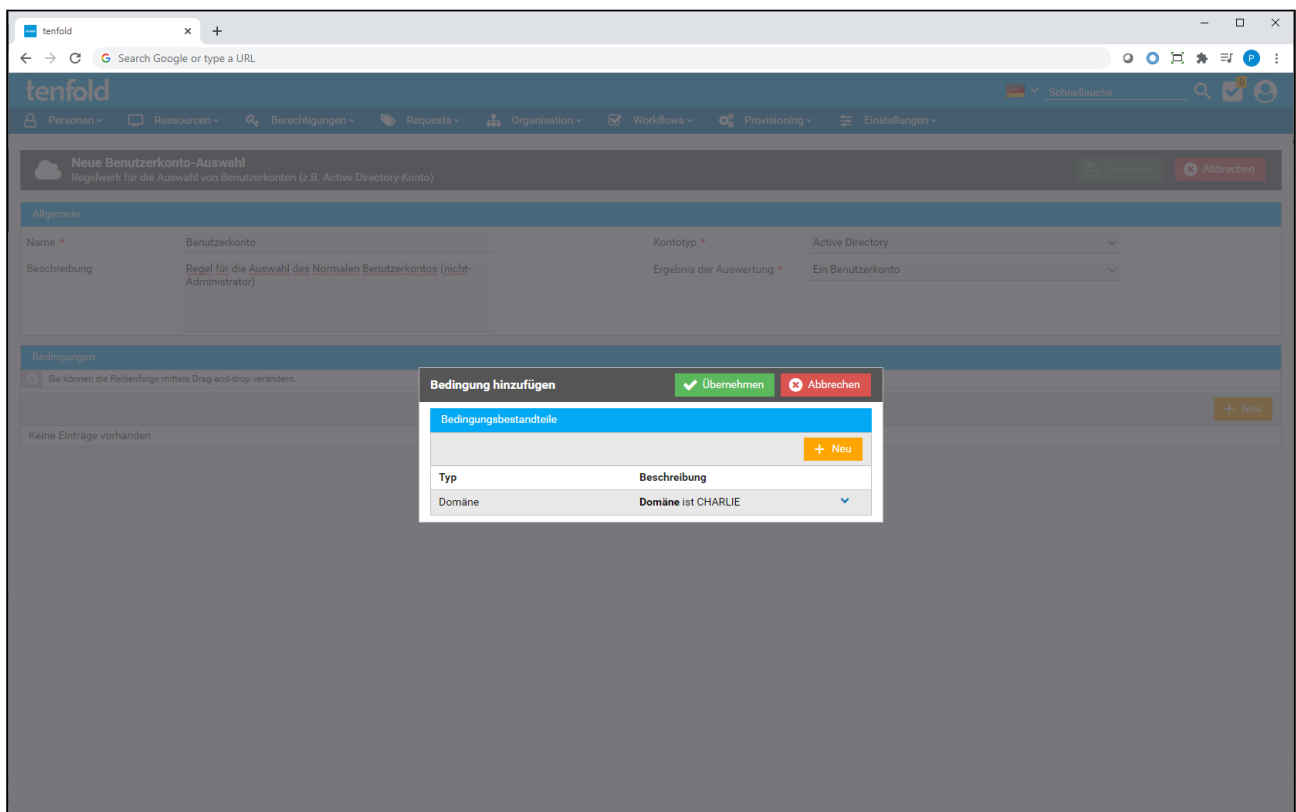
[+ Neu](#)

Keine Einträge vorhanden

Im Bereich *Allgemein* lassen sich folgende Einstellungen treffen:

Einstellung	Beschreibung
Name	Der Name dieser Regel. Diese wird zur Anzeige in tenfold genutzt.
Beschreibung	Eine rein informative Beschreibung der Regel. Verwenden Sie diese um detaillierter zu beschreiben wofür diese Regel verwendet wird.
Kontotyp	Legt fest, für welche Art von Konto diese Regel ausgelegt ist. Die Auswahlmöglichkeiten sind <i>Active Directory</i> und <i>Microsoft 365</i> . Von dieser Auswahl hängen die möglichen Bedingungen ab.
Ergebnis der Auswertung	Legt fest, ob nur das erste gefundene Konto ausgewählt werden soll oder alle gefundenen Konten.

Nachdem die allgemeinen Einstellungen gemacht wurden, müssen die Bedingungen festgelegt werden. Mit den Bedingungen wird die Auswahl der Benutzerkonten eingestellt.
Zum Hinzufügen einer neuen Bedingung klicken Sie auf die Schaltfläche *Neu*.



Im daraufhin erscheinenden Dialog können Sie nun mehrere Bestandteile zu der Bedingung hinzufügen. Damit eine Bedingung als erfüllt gilt, müssen alle darin enthaltenen Bestandteile erfüllt sein. Je nach ausgewähltem Kontotyp können Sie aus folgenden Bestandteilen auswählen:

Kontotyp	Bestandteil	Beschreibung
Active Directory	Domäne	Das Konto muss sich in der ausgewählten Active Directory Domäne befinden.
Active Directory	Kategorie	Das Konto muss in tenfold einer bestimmten Kategorie (User, Administrator, Functional user account, Service user account) zugeordnet sein.
Active Directory	OU	Das Konto muss sich in einer bestimmten Organisationseinheit oder einer darunter liegenden Organisationseinheiten befinden.
Microsoft 365	Microsoft 365-Mandant	Das Konto muss sich auf einem bestimmten Mandanten befinden.
Microsoft 365	Active Directory Benutzerkonto-Auswahl	Das Microsoft 365-Konto muss durch den Azure AD Connect mit einem Konto der lokalen Domäne verknüpft sein, welches durch eine Active Directory Benutzerkonto-Auswahl gefunden wird.
Active Directory, Microsoft 365	Kontostatus	Legt fest, ob das Konto aktiv oder inaktiv sein muss.

Kontotyp	Bestandteil	Beschreibung
Active Directory, Microsoft 365	Code Snippet	Das Ergebnis wird durch ein Snippet bestimmt. Dieser Bestandteil kann verwendet werden, wenn andere Bestandteile unzureichend sind. Wenden Sie sich bitte an Ihren Implementierungspartner damit dieser Sie beim Anlegen dieser Bestandteile unterstützt.

Sie können mehrere Bedingungen zu der Auswahlregel hinzufügen. Sie können die Reihenfolge angelegter Bedingungen per Drag & Drop verändern. Die Reihenfolge hat Auswirkungen auf die Auswertung der Regeln. Nähere Details dazu wie Bedingungen verarbeitet werden, finden Sie unter [Auswertung von Regeln](#) (see page 577).

Zuletzt klicken Sie auf *Speichern*, um die soeben erstellte Regel zu speichern.

Leere Auswahl-Regeln

Eine Auswahl-Regel muss über zumindest eine Bedingung verfügen bevor sie gespeichert werden kann. Leere Auswahlregeln werden nicht unterstützt.

13.4.2 Vorhandene Regel bearbeiten od. löschen

Um eine bereits bestehende Regel zu bearbeiten, navigieren Sie im Menü auf die Seite Provisioning > Regelwerke > Benutzerkonto-Auswahl. Wählen sie daraufhin im Aktionsmenü der gewünschten Regel die Aktion *Bearbeiten*.

Dort angeleant, folgen Sie denselben Schritten wie beim Anlegen einer neuen Regel.

Zum Löschen einer Regel wählen Sie im Aktionsmenü der entsprechenden Regel die Aktion *Löschen*. Sollte die Regel in Verwendung sein, erhalten Sie eine Fehlermeldung welche Ihnen anzeigt, an welchen Stellen die Regel verwendet wird. Die Regel muss manuell von allen Stellen entfernt werden, bevor sie gelöscht werden kann.

13.4.3 Auswertung von Regeln

Regeln zur Benutzerkonto-Auswahl werden immer im Kontext einer Person ausgeführt. Wird zum Beispiel einer Person ein Profil zugeordnet und in diesem Profil befinden sich Microsoft 365-Gruppen so muss entschieden werden, welchem Microsoft 365-Konto die Gruppe hinzugefügt wird. Hierfür kann in einem Profil eine Regel zur Benutzerkonto-Auswahl hinterlegt werden. Zusätzlich zu allen in der Regel hinterlegten Bedingungen müssen gefundene Konten auch der Person zugeordnet sein.

Personen mit nur einem Konto

Die Regeln werden auch dann überprüft, wenn die betroffene Person nur ein Konto besitzt, da es sein könnte, dass auf dieses Konto keine der Bedingungen zutrifft.

Die Bedingungen werden in der Reihenfolge ausgewertet, in welcher sie in der Tabelle hinterlegt sind. Je nachdem, welche Option in der Einstellung *Ergebnis der Auswertung* gewählt wurde, erhalten Sie nun ein oder mehrere Konten als Ergebnis dieser Regel.

Einstellung	Ergebnismenge
Ein Benutzerkonto	Liefert das erste Benutzerkonto der ersten zutreffenden Regel zurück.
Alle zutreffenden Benutzerkonten	Liefert alle Benutzerkonten zurück, von allen Regeln welche Ergebnisse liefern.

Beispiel 1

Eine Person hat drei Benutzerkonten.

- MeineDomain.de\MeineOrganisation\Benutzer\MeinBenutzer (Normales Konto)
- MeineDomain.de\MeineOrganisation\Administratoren\Adm.MeinBenutzer (Administrator Konto)
- FremdDomain.de\FremdeOrganisation\Benutzer\MeinGastAdministrator (Administrator)

Eine Regel wurde erstellt, welche ein Konto liefert und folgende Bedingungen enthält:

1. Domäne ist MeineDomain.de **UND** OU ist MeineDomain.de\MeineOrganisation\Benutzer
2. Domäne ist MeineDomain.de **UND** Kontotyp ist Normaler Benutzer

Das Ergebnis dieser Regel lautet: *MeineDomain.de\MeineOrganisation\Benutzer\MeinBenutzer (Normales Konto)*

Die erste Bedingung liefert bereits das Konto, da es in der gewünschten OU liegt. Läge das Konto in einer anderen OU würde, es immer noch durch die zweite Bedingung gefunden werden, da es in tenfold als Normales Benutzerkonto markiert ist.

Beispiel 2

Eine Person hat drei Benutzerkonten.

- MeineDomain.de\MeineOrganisation\Benutzer\MeinBenutzer (Normales Konto)

- MeineDomain.de\MeineOrganisation\Administratoren\Adm.MeinBenutzer (Administrator Konto)
- FremdDomain.de\FremdeOrganisation\Benutzer\MeinGastBenutzer

Eine Regel wurde erstellt, welche Alle Konten liefert und folgende Bedingungen enthält:

1. Domäne ist FremdDomain.de
2. Kontotyp ist Administrator

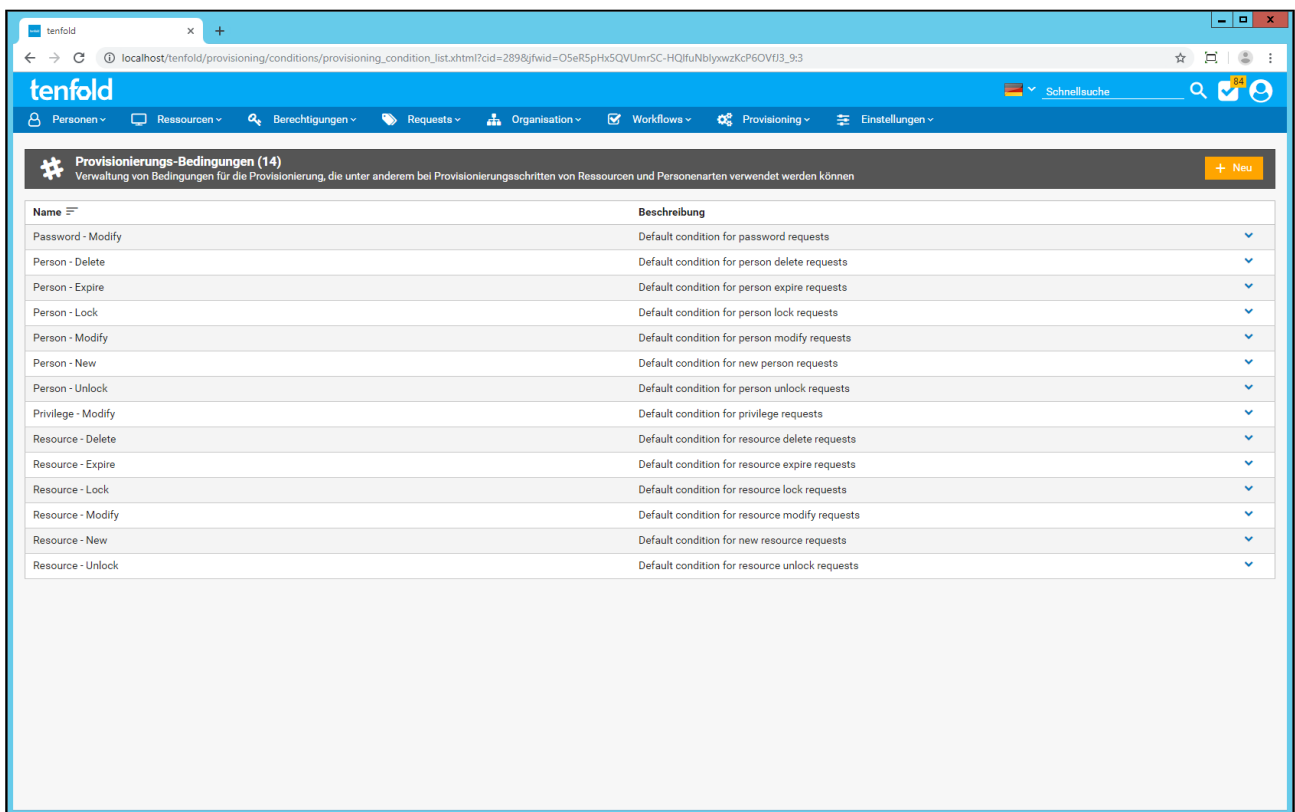
Das Ergebnis dieser Regel lautet: *MeineDomain.de\MeineOrganisation\Benutzer\MeinBenutzer* (Normales Konto) und *MeineDomain.de\MeineOrganisation\Administratoren\Adm.MeinBenutzer* (Administrator Konto)

Keine Regel trifft zu

Sollte es vorkommen, dass für eine Ausgewählte Regel, kein Konto gefunden wird, welches zu einer der Bedingungen passt, so geht der betroffene Request in eine Wartestellung, bis der betroffenen Person ein entsprechendes Konto zugeordnet wird.

13.5 Bedingungen

Bedingungen haben den Zweck, in Provisionierungen bestimmte Schritte nur dann auszuführen, wenn der Request, auf Basis dessen provisioniert werden soll, bestimmte Bedingungen erfüllt. Diese Bedingungen können an dieser Stelle zentral verwaltet werden, damit sie anschließend - ohne die Einstellungen mehrfach angeben und in weiterer Folge ändern zu müssen - verwendet werden können. Jede Bedingung besteht dabei aus einem oder mehreren Elementen, die jeweils einen Teil der Bedingungen abfragen. Damit eine Bedingung als erfüllt gilt, müssen alle Elemente der Bedingung erfüllt sein. Wird ein Element nicht erfüllt, so gilt die gesamte Bedingung als nicht erfüllt.



Zur Verwaltung der Bedingungen gelangen Sie über das Menü *Provisioning* > *Regelwerke* > *Provisionierungsbedingungen*.

Benötigte Berechtigung

Für den Zugriff auf diese Seite wird die tenfold-Berechtigung "Manage provisioning conditions" (8450) benötigt.

13.5.1 Einzelbeschreibung

Die meisten Elemente der Bedingungen sind anhand der Informationen aus den Feldmappings relativ selbsterklärend (siehe auch [Feldmappings](#)(see page 556)). Die wichtigsten Auswahlmöglichkeiten sind hier zusätzlich beschrieben:

Feld	Auswahl	Beschreibung
Modus		
	Bedingungen	Die Bedingung kann anhand von Auswahlfeldern formuliert werden.

	Code Snippet	Sind die Möglichkeiten dessen erschöpft, gibt es die Möglichkeit über "Code Snippet" ein Snippet zu hinterlegen. Das Code Snippet erhält einen Parameter "request" vom Datentyp <i>Request</i> (siehe Datentypen(see page 608)) und muss anschließend den boolean "true" oder "false" liefern, je nachdem, ob die Bedingung erfüllt ist, oder nicht. Wird eine Exception geworfen und im Snippet nicht gefangen, gilt die Bedingung als nicht erfüllt.
Request-Modus		
	*	Über diese Auswahl kann eingeschränkt werden, welcher Modus der Request aufweisen muss, damit die Bedingung erfüllt ist. Außerdem steuert der Modus die Verfügbarkeit der nachfolgenden Felder.
Request-Typ		
	*	Über diese Auswahl kann eingeschränkt werden, welchen Typ der Request aufweisen muss, damit die Bedingung erfüllt ist. Außerdem steuert der Typ die Verfügbarkeit der nachfolgenden Felder. Nicht jeder Request-Modus erlaubt auch jeden Request-Typ. Über die Request-Typ-Bedingung kann abgefragt werden, ob es sich beim Typ genau um diesen Typ handeln muss, oder ob es sich um genau diesen Typ nicht handeln darf.
Ereignis		
	Provisioning	Die Prüfung und Durchführung des Provisioning-Schritts, mit welchem die Bedingung verknüpft ist, erfolgt bei der Provisionierung, also beim Durchführen des Requests.
	Before Close	Das Ereignis erfolgt, wenn der Request geschlossen wird, bevor andere Aktionen beim Schließen angestoßen werden.
	Before Cancel	Das Ereignis erfolgt, wenn der Request abgebrochen wird, bevor andere Aktionen beim Abbrechen angestoßen werden.
Request-Quelle		
	*	Über diese Auswahl kann eingeschränkt werden, aus welcher Quelle der Request stammen muss, damit die Bedingung erfüllt ist. Es kann zum Beispiel abgefragt werden, ob die Request-Quelle ein HR-System ist. Diese Request-Quelle kann wiederum beim Import Plugin (siehe Import Plugin(see page 710)) gesetzt worden sein. Über die Request-Quelle-Bedingung kann abgefragt werden, ob es sich beim Typ genau um diese Quelle handeln muss, oder ob es sich um genau diese Quelle nicht handeln darf.

Begründung		
	*	Es kann abgefragt werden, ob der Request genau diese Begründung aufweist, oder genau diese Begründung nicht aufweist (Begründung-Bedingung).
Personenfeld		
	*	Diese Auswahl ist nur verfügbar, wenn zuvor im Request-Modus "Personendaten" ausgewählt wurde. Hier kann ein spezielles Personenfeld gewählt werden, auf welches reagiert werden soll.
Ressource		
	*	Die Bedingung ist nur dann erfüllt, wenn sich der Request auf die ausgewählte Ressource bezieht. Diese Option ist sowohl im Modus "Ressource", als auch im Modus "Anwendungsberechtigung" verfügbar.
Ressourcenkategorie		
	*	Die Bedingung ist nur dann erfüllt, wenn sich der Request auf eine Ressource bezieht, welche aus der ausgewählten Ressourcenkategorie stammt. Diese Option ist sowohl im Modus "Ressource", als auch im Modus "Anwendungsberechtigung" verfügbar.
Option		
	*	Mit dieser Einstellung kann auf den Inhalt von Ressourcen-Optionen geprüft werden. Wählen Sie hier die Option aus, welche überprüft werden soll. Hinweis: An dieser Stelle stehen sämtliche eingetragenen Optionen zur Verfügung. Sollten Sie eine Einschränkung auf eine Ressource tätigen, welche diese Option nicht enthält, kann die Bedingung nie erfüllt werden.
Berechtigung		
	*	Es kann eine bestimmte Berechtigung gewählt werden. Mit dem Feld "Berechtigungs-Typ" kann anschließend definiert werden, ob der Request die Berechtigung erteilt, entzieht, oder ob dies unerheblich ist.
Reagieren auf		
		Diese Option steht mehrfach zur Verfügung, zum Beispiel bei der Änderung von Personenfeldern im Modus "Personendaten", aber auch bei der Änderung von Optionen im Modus "Ressource"

	Wertänderung	Jegliche Wertänderung führt dazu, dass die Bedingung erfüllt ist.
	Änderung auf bestimmten Wert	Nur, wenn der Wert des Feldes auf einen bestimmten Wert geändert wird, ist die Bedingung erfüllt. Ob vorher ein Wert vorhanden ist oder nicht ist unerheblich.
	Änderung von Leerwert auf Wert	Nur, wenn der Wert des Feldes zuvor leer war und nunmehr nicht mehr leer ist, ist die Bedingung erfüllt. Welcher Wert der neue Wert ist ist unerheblich.
	Änderung von Leerwert auf bestimmten Wert	Nur, wenn der Wert des Feldes auf einen bestimmten Wert geändert wird und der Wert zuvor leer war, ist die Bedingung erfüllt.
	Änderung von Wert auf Leerwert	Nur, wenn der Wert des Feldes auf leer geändert wird und der Wert zuvor nicht leer war, ist die Bedingung erfüllt.
	Wert bleibt gleich	Nur, wenn der Wert sich nicht ändert, ist die Bedingung nicht erfüllt.
	Feld hat bestimmten Wert	Wenn das Feld einen bestimmten Wert aufweist, der sich durch den Request jedoch nicht ändern darf (sonst trifft eine der obigen Bedingungen zu), ist die Bedingung erfüllt.
	Feld hat keinen Wert	Trifft zu, wenn das ausgewählte Feld leer ist.
	Feld hat Wert	Trifft zu, wenn das ausgewählte Feld nicht leer ist.

13.5.2 Personenkreise

Zusätzlich zu den jeweiligen Einstellungen für die Art der Bedingung kann für jeden Request-Modus (außer Personendaten) eine Einschränkung nach Personenkreis konfiguriert werden. Wird eine Einschränkung des Personenkreises getroffen, so gilt die Bedingung nur dann als erfüllt, wenn, zusätzlich zu allen anderen Konfigurationen, die Zielperson des entsprechenden Requests in den eingestellten Personenkreis fällt. Die Einschränkung findet mittels Feldregeln statt (siehe [Feldregeln](#)(see page 562)).

Personenkreis für Personenänderungen

Da die Personendaten in den Einstellungen der Bedingungen für Personendaten-Requests direkt abgefragt werden können, ist eine Einschränkung des Personenkreises für diesen Request-Modus überflüssig und wird daher nicht angeboten.

Sollten Sie in einer andere Bedingung einen anderen Request-Modus als "Personendaten" ausgewählt haben, erscheint unterhalb des Bereichs "Bedingung" der Bereich "Personenkreis". Hier haben Sie folgende Einstellungsmöglichkeiten:

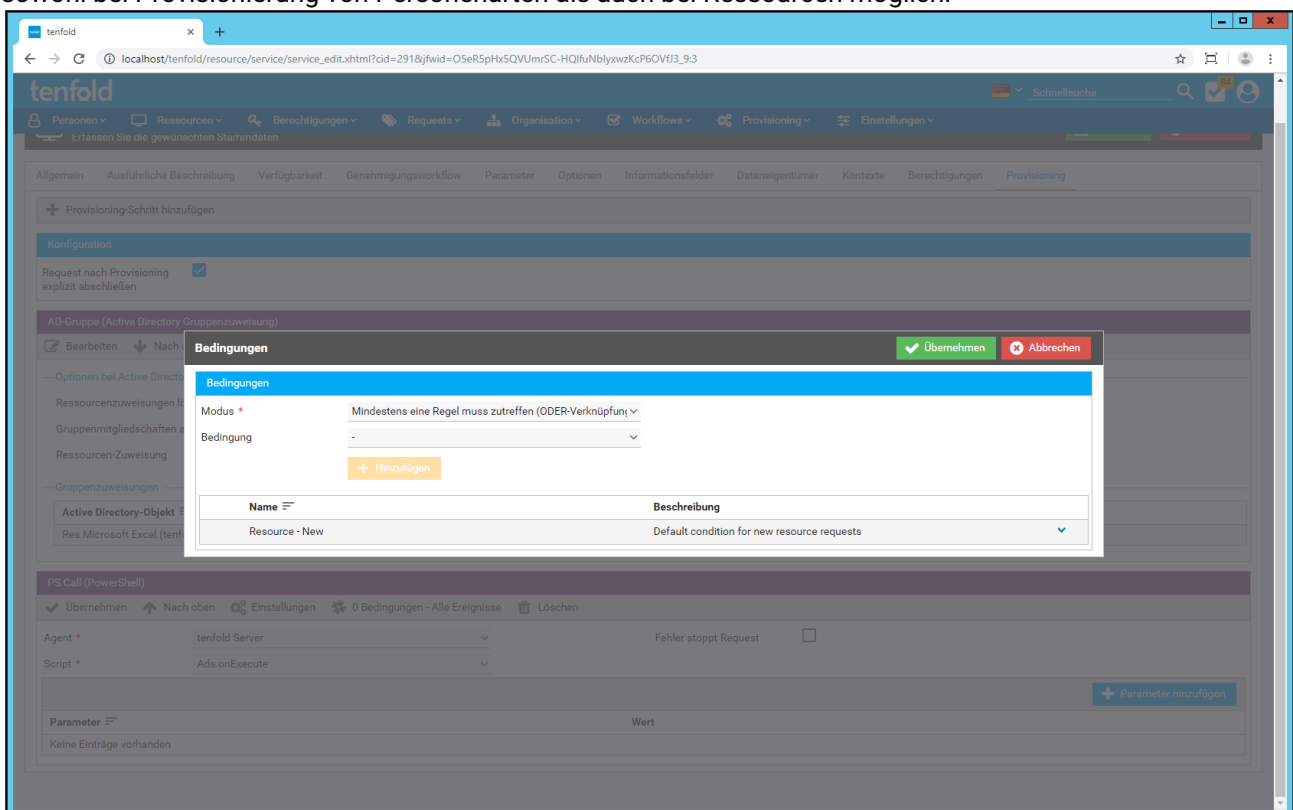
Einstellung	Beschreibung
Einschränken	Ist diese Einstellung aktiv, so können Einschränkungen auf den Personenkreis getroffen werden. Ist sie nicht aktiv, dann trifft die Bedingung auf alle Personen zu.
Modus	Mit dieser Einstellung legen Sie fest, ob zumindest eine der ausgewählten Feldregeln zutreffen muss oder ob alle ausgewählten Feldregeln zutreffen müssen. Sollte nur eine Feldregel ausgewählt werden ist diese Einstellung ohne Bedeutung.
Feldregeln	Wählen Sie hier eine oder mehrere Feldregeln aus, welche auf Personen zutreffen müssen, damit diese Bedingung als erfüllt gilt.

Request-Modus Personendaten

Da das Abfragen auf die Daten einer Person sonst nur im Modus "Personendaten" zur Verfügung steht, können Sie über die Personenkreiseinschränkungen auch in jedem anderen Request-Modus Personendaten abfragen. Damit kann, zum Beispiel, die Provisionierung eines Plugins bei der Zuweisung einer Ressource auf Personen mit eingetragener E-Mail-Adresse eingeschränkt werden.

13.5.3 Verwendung

Die zuvor erstellte Bedingung kann nun mit einem Provisionierungsschritt verknüpft werden. Eine Nutzung ist sowohl bei Provisionierung von Personenarten als auch bei Ressourcen möglich.



Es können für jeden Schritt mehrere Bedingungen hinzugefügt werden, wobei definiert werden kann, ob alle dieser Bedingungen zutreffen müssen oder, ob es genügt, dass eine der ausgewählten Bedingungen zutrifft.

Warnung

Achtung: Nicht alle Plugins unterstützen die Verwendung von Bedingungen! Ob Bedingungen unterstützt werden ist davon abhängig, ob der hinzugefügte Schritt den Button "Bedingungen" beinhaltet oder nicht.

Darüber hinaus unterstützen nicht alle Plugins alle Bedingungsarten. Zum Beispiel könnte ein Plugin keine Bedingungen unterstützen, die auf Personenänderungen verweisen. In diesem Fall werden Sie nach der Auswahl der Bedingung auf diesen Umstand hingewiesen.

13.5.4 Anwendungsbeispiel

Wird bei einer Person das Feld "Mobiltelefon" von leerem Inhalt auf einen Wert gesetzt, so soll ein Powershell-Script ausgeführt werden. Dabei sind nachfolgende Schritte notwendig.

Allgemein	
Name *	Mobile changes ...
Beschreibung	This condition is true, when the mobile phone number changes from empty to a value.

Bedingungen	
Modus *	Bedingungen
Request-Modus *	Personendaten
Request-Typ	Änderung
Request-Typ-Bedingung	Request-Typ muss 'Änderung' sein
Ereignis	Provisioning
Request-Quelle	tenfold
Request-Quellen-Bedingung	Request-Quelle muss 'tenfold' sein
Begründung	*
Personenfeld	Mobiltelefon
Reagieren auf *	Änderung von Leerwert auf Wert

1. Anlage des Scripts (Provisioning > Scripts)
2. Anlage einer Bedingung mit folgendem Inhalt (siehe Screenshot):
 - a. Modus: Bedingung
 - b. Request-Modus: Personendaten
 - c. Request-Typ: Änderung
 - d. Request-Typ-Bedingung: Request-Typ muss Änderung sein
 - e. Ereignis: Provisioning
 - f. Request-Quelle: tenfold
 - g. Request-Quellen-Bedingung: Request-Quelle muss tenfold sein

- h. Begründung: *
 - i. Personenfeld: Mobiltelefon
 - j. Reagieren auf: Änderung von Leerwert auf Wert
3. Anlage eines Provisioning-Schritts bei der gewünschten Personenart
 4. Verknüpfen dieses Schritts mit der zuvor angelegt Bedingung

13.6 Regeln für Benutzernamen

13.6.1 Allgemeines

Wenn tenfold, über entsprechende Plugins, Benutzerkonten in Fremdsystemen anlegt, so müssen für diese Konten Benutzernamen vergeben werden. Um dem Administrator diese Aufgabe zu erleichtern gibt es die Möglichkeit, Benutzernamen automatisch generieren zu lassen. Die Generierung von Benutzernamen folgt dabei spezifisch definierten Regeln. Diese Regeln können in tenfold hinterlegt werden.

13.6.2 Verwaltung

Die Funktion, um diese Regeln zu konfigurieren, ist über das Menü *Provisioning > Regelwerke > Benutzernamen* erreichbar.

Benötigte Berechtigung

Für die Verwaltung der Regeln für Benutzernamen ist die Systemberechtigung "Manage Username Rules" (8094) erforderlich

The screenshot shows the 'Regeln für Benutzernamen' configuration page in the tenfold web interface. The page has a blue header with the tenfold logo and navigation menu. The main content area is titled 'Regeln für Benutzernamen' and includes a 'Speichern' button. Below the title, there is a table for rules and a decision table for field rules.

Name	Modus	Anzahl Buchstaben Vorname	Anzahl Buchstaben Nachname	Ressourcen
Default	Konfiguration	1	7	Alle Ressourcen
Externe Mitarbeiter	Konfiguration	1	5	Alle Ressourcen

Decision Table

Sie können die Reihenfolge mittels Drag-and-drop verändern.

Feldregel	Benutzernamen-Regel
Personentyp ist Mitarbeiter	Default
Personentyp ist Externe Benutzer	Externe Mitarbeiter

Im oberen Bereich der Maske werden die Regeln, nach denen ein Benutzername generiert wird, festgelegt. Im unteren Bereich kann, auf Basis von Feldregeln, festgelegt werden, in welchen Situationen (für welche Personenarten, Abteilungen oder Systeme) welche Regel zur Anwendung kommen soll.

13.6.3 Verwaltung der Regeln

Neue Regeln können über den Button "Hinzufügen" angelegt werden. Bestehende Regeln können über das Kontextmenü mit der Option "Bearbeiten" verändert werden. Regeln, die nicht mehr benötigt werden, können über die Option "Löschen" entfernt werden. Dies ist allerdings nur dann möglich, wenn die Regel nicht mehr angewendet wird. Das bedeutet, sie darf nicht in der Tabelle unterhalb verwendet werden.

Regeleinstellungen

Folgende Einstellungen können für eine Regel festgelegt werden:

Einstellung	Beschreibung
Name	Dient lediglich zur Anzeige auf der Oberfläche

Einstellung	Beschreibung
Modus	<p>Hier kann zwischen zwei grundlegenden Einstellungen unterschieden werden:</p> <p>Konfiguration</p> <ul style="list-style-type: none"> • In dieser Einstellung können die Optionen komfortabel auf der Oberfläche konfiguriert werden. Sofern die gewünschte Logik hiermit abbildbar ist, wird dieser Weg empfohlen. • Die nachfolgend beschriebenen Einstellung sind nur verfügbar, wenn der Modus auf "Konfiguration" eingestellt wurde. <p>Snippet</p> <ul style="list-style-type: none"> • Sollte sich die gewünschte Logik nicht abbilden lassen, kann auf Snippet umgestellt werden. • Dazu muss per Script ein Benutzername generiert werden. Das Script erhält die Daten zur Person über den Parameter "Person". • Der generierte Benutzername muss vom Script über den "return" Befehl retourniert werden. <p>Achtung: Die Prüfung auf Duplikate in allen zu prüfenden Fremdsystemen muss in diesem Fall manuell erfolgen!</p>
Aufbereitung Vorname	<p>Es kann hier konfiguriert werden, dass der Inhalt des Personenfeldes "Vorname" bei der Generierung aufbereitet wird. Folgende Optionen stehen zur Verfügung:</p> <ul style="list-style-type: none"> • Keine: Es erfolgt keine Aufbereitung • Sonderzeichen ersetzen: Es werden die deutschen Umlaute ersetzt ("ä" wird zu "ae", "ö" zu "oe", "ü" zu "ue"). • Snippet: Die Aufbereitung erfolgt per Script. Der Eingangswert wird unter der Variable "value" bereitgestellt. Der aufbereitete Wert muss über "return" retourniert werden.
Aufbereitung Nachname	<p>Analog zum vorangegangenen Punkt, allerdings für das Personenfeld "Nachname".</p>
Schreibweise	<p>Mit dieser Option kann die Groß- und Kleinschreibung in der gewünschten Weise forciert werden.</p>
Schwarze Liste	<p>Wird diese Option aktiviert, so kann man anschließend eine Personenliste (siehe Personenlisten(see page 116)) angeben. Alle Einträge aus der Personenliste, die einen Benutzernamen eingetragen haben, werden von der Generierung ausgeschlossen.</p>

Einstellung	Beschreibung
Betroffene Ressource	<p>Diese Option wird dazu genutzt, um einzustellen, welche Systeme nach etwaigen Duplikaten abgefragt werden. So ist es beispielsweise möglich, einen systemübergreifend einheitlichen Benutzernamen zu generieren, da ein Duplikat in nur einem System automatisch zur Eskalation und damit zur Generierung einer Alternative führt. Es kann unterschieden werden zwischen:</p> <ul style="list-style-type: none"> • Alle Ressourcen: Es werden alle zutreffenden Ressourcen, also alles konfigurierten Fremdsysteme, abgefragt. • Bestimmte Ressourcen: Es kann individuell ausgewählt werden, welche Systeme abgefragt werden sollen. <p>Abgefragt werden können nur jene Ressourcen, die:</p> <ul style="list-style-type: none"> • Im Provisioning eines oder mehrere Plugin(s) nutzen • Zumindest eines der Plugins die Funktion bietet, das ihm zugrunde liegende Fremdsystem auf Benutzernamen zu prüfen <p>Mit der Option "tenfold-Benutzernamen überprüfen" können zusätzlich die Hauptbenutzernamen aus tenfold in die Prüfung mit aufgenommen werden. Dabei können folgende Varianten gewählt werden:</p> <ul style="list-style-type: none"> • Alle: Es werden die Hauptbenutzernamen von allen Personen in tenfold geprüft, egal ob aktiv oder gelöscht. • Nur aktive Benutzername: Es werden nur die Hauptbenutzernamen von aktiven Personen geprüft. • Nur gelöschte Benutzernamen: Es werden nur die Hauptbenutzernamen von gelöschten Personen geprüft. • Keine: Es findet keine Prüfung der Hauptbenutzernamen statt <div data-bbox="555 1234 1426 1424" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Tip</p> <p>Diese Funktion dient primär dazu, zu verhindern, dass historische Benutzernamen (die bereits einmal zugewiesen waren) nochmals verwendet werden.</p> </div>
Bestandteile	<p>Hier kann festgelegt werden, aus welchen Bestandteile sich der Benutzername zusammensetzt.</p> <ul style="list-style-type: none"> • Durch das An- und Abwählen unterschiedlicher Bestandteile können diese aktiviert und deaktiviert werden. Wird beispielsweise der Vorname deselektiert, so stehen die Optionen für den Vornamen auch nicht zur Verfügung. • Die Reihenfolge von Vor- und Nachname kann verändert werden. • Das Präfix ist immer der erste Bestandteil und das Postfix der letzte Bestandteil. Ihre Reihenfolge kann nicht verändert werden.
Präfix	<p>Mit dieser Option kann ein gewünschtes Präfix festgelegt werden. Beispielsweise könnte für Konten von externen Mitarbeitern "ext-" angegeben werden.</p>

Einstellung	Beschreibung
Vorname	<ul style="list-style-type: none"> • Es kann entweder der gesamte Inhalt des Personenfeldes "Vorname" oder nur eine bestimmte, maximale Zeichenanzahl verwendet werden. • Diese ist in der nachfolgenden Option "Anzahl" einzutragen. • Ist der Vorname kürzer als die maximale Zeichenanzahl, so wird die ganze Zeichenkette verwendet.
Vorname-Teil erhöhen	Wenn diese Option aktiviert ist kann der Generator den Anteil der Buchstaben aus dem Vornamen über die definierte Anzahl hinaus erhöhen, damit der Benutzername der maximalen Länge entspricht.
Trennzeichen	Wenn zwischen Vor- und Nachname ein Trennzeichen verwendet werden soll, so kann dieses hier eingegeben werden. Um kein Trennzeichen zu verwenden, lassen Sie die Option leer.
Nachname	Analog zum Punkt "Vorname", allerdings für die Behandlung des Personenfeldes "Nachname".
Nachname-Teil erhöhen	Wenn diese Option aktiviert ist kann der Generator den Anteil der Buchstaben aus dem Nachnamen über die definierte Anzahl hinaus erhöhen, damit der Benutzername der maximalen Länge entspricht.
Maximale Länge-Modus	Bei der Verwendung der Option "Ganzer Name" in den Einstellungen "Vorname" und "Nachname" kann es vorkommen, dass Benutzernamen generiert werden, welche nicht in die entsprechenden Felder des Zielsystems hineinpassen (Beispiel: Active Directory sAMAccountName darf maximal 20 Zeichen enthalten). Um dies zu verhindern, kann eine maximale Länge des zu erzeugenden Benutzernamens erzwungen werden. Wählen Sie hierfür in dieser Einstellung die Option "Benutzerdefiniert". Mit der Option "Unbegrenzt" werden Benutzernamen beliebiger Länge erzeugt.
Abkürzungsmodus	Legt fest, ob zuerst Zeichen des Vornamens oder des Nachnamens entfernt werden sollen, um einen Benutzernamen auf die maximal erlaubte Anzahl von Zeichen zu kürzen.
Maximale Länge	Legt eine Anzahl an Zeichen fest, welche ein gültiger Benutzername maximal haben darf.

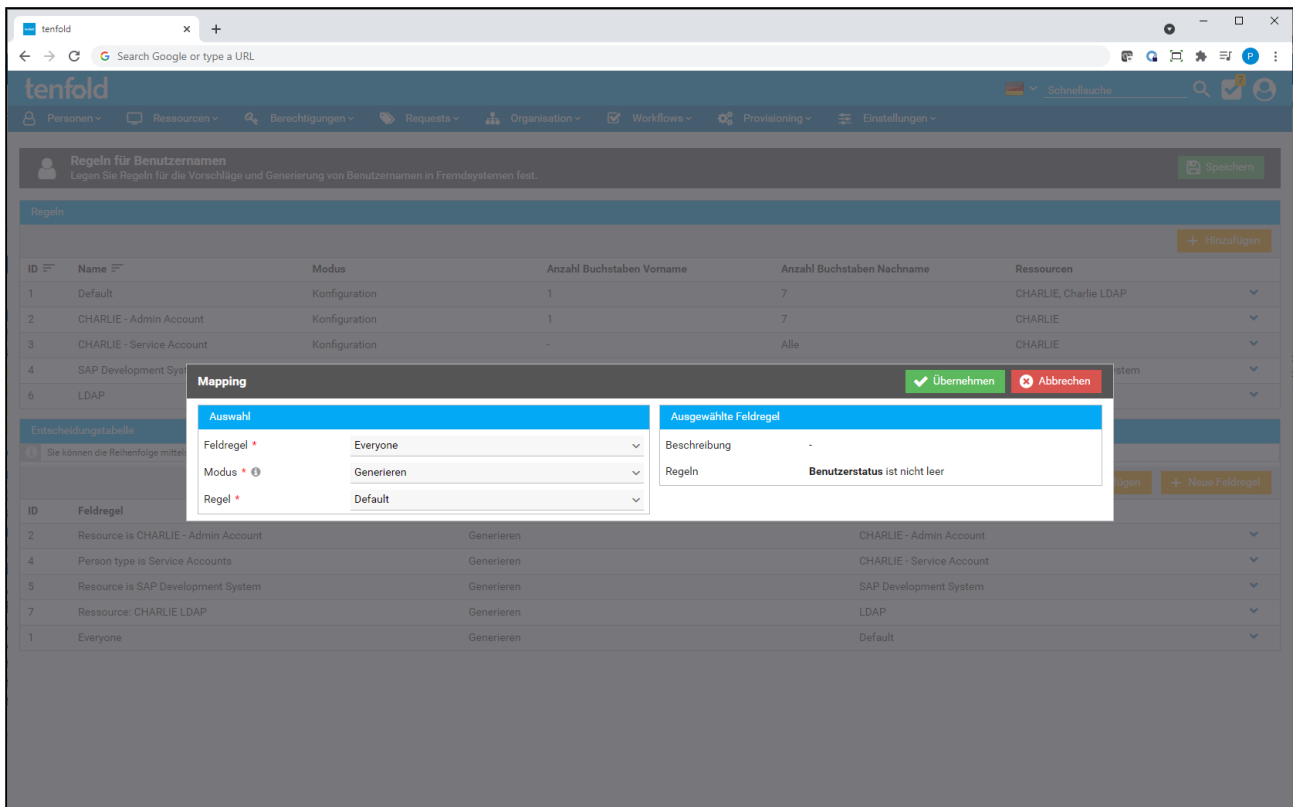
Einstellung	Beschreibung
Eskalationsschema 1	<p>Das Eskalationsschema kommt zum Tragen, wenn ein Benutzername nach den vorhergehenden Regeln erzeugt wurde, sich aber bei der Prüfung (siehe Option "Betroffene Ressourcen") herausstellt, dass dieser Benutzername bereits verwendet wird.</p> <ul style="list-style-type: none"> • Laufende Nummer: Es wird, beginnend bei 1, eine laufende Nummer an den Namen angehängt. Ist der Benutzername mit angehängter 1 bereits vergeben, wird mit 2 fortgefahren und so weiter. • Weiterer Buchstabe Vorname/Nachname: Es wird - statt der definierten maximalen Anzahl an Buchstaben - ein weiterer Buchstabe des Vornamens/Nachnamens verwendet (nur für bestimmte Zeichenzahl bei Namen) . • Buchstabe Vorname/Nachname entfernen: Es wird ein Buchstabe des Vornamens/Nachnamens entfernt (nur für "Ganzer Name"), bis der Name leer ist. • Buchstabe Vorname bis auf den letzten entfernen: Es wird ein Buchstabe des Vornamens/Nachnamens entfernt, bis nur noch ein Buchstabe des Namens übrig geblieben ist (nur für "Ganzer Name").
Eskalationsschema 2	<p>Dieses Schema ist nur verfügbar, wenn das Eskalationsschema 1 nicht "Laufende Nummer" lautet (denn dieses Schema generiert in jedem Fall einen eindeutigen Benutzernamen - es stellt sich nur die Frage nach der Höhe der laufenden Nummer).</p> <p>Dieses Schema wird dann verwendet, wenn alle Möglichkeiten des ersten Eskalationsschemas bereits erfolglos ausprobiert wurden.</p>
Eskalationsschema 3	<p>Ein weiteres Eskalationsschema analog zu "Eskalationsschema 2". Dieses Schema ist nur verfügbar, wenn bei Vor- oder Nachname die Option "Ganzer Name" ausgewählt wurde.</p>
Suffix	<p>Analog zur Einstellung "Präfix", allerdings für das Ende des generierten Benutzernamens</p>
Maximale Länge von (X) Zeichen darf überschritten werden	<p>Diese Einstellung bewirkt, dass der Benutzername nicht über die maximal denkbare Größe (aufgrund der Einstellungen, die hinterlegt sind) anwachsen darf. Stattdessen wird der Benutzername, auf Kosten bestimmter Bestandteile, gekürzt.</p> <p>Beispiel:</p> <p>Wird das Eskalationsschema "Laufende Nummer" genutzt und wurde für den Benutzernamen <i>mmusterm</i> ein Duplikat festgestellt, würde, sofern diese Option nicht gesetzt ist, nach der Eskalation <i>mmusterm1</i> generiert werden. Wird die Option allerdings gesetzt, sodass die maximale Länge von 8 Zeichen nicht überschritten werden darf, so wird der letzte Bestandteil (in diesem Fall der Nachname) gekürzt und der Benutzername <i>mmuster1</i> generiert.</p>

Achtung

Wird eine Regel geändert und gespeichert, so wirken sich die Änderungen nur auf neu generierte Benutzernamen aus. Bestehende Benutzernamen sind von der Änderung nicht betroffen.

13.6.4 Anwendungsbereich der Regeln

Zweck



Die Entscheidungstabelle im unteren Bereich der Maske legt fest, in welchen Situationen welches Regelwerk verwendet werden soll. So kann, auf Basis von Feldregeln beispielsweise, unterschieden werden:

- dass für Fremdsystem unterschiedliche Regeln gelten sollen (Active Directory könnte nach der Regel *Vorname.Nachname* und SAP nach der Regel *VNNNNNNN* funktionieren)
 - Unterscheidung nach dem Feld "Ressource"
- dass für Personenarten verschiedene Regeln gelten (Active Directory-Benutzer interne Mitarbeiter werden nach der Regel *Vorname.Nachname* erzeugt, externe als *Ext-Vorname.Nachname*)
 - Unterscheidung nach dem Feld "Personenart"
- dass für mehrere unterschiedliche Windows-Domains unterschiedliche Regeln gelten
 - Unterscheidung nach dem Feld "Ressource" (jede Domain wird als eine Ressource abgebildet - siehe auch [Verwaltung der Fileserver-Berechtigungen](#)(see page 269))
- dass für Standorte des Unternehmens verschiedene Präfixe verwendet werden
 - Unterscheidung nach dem Personenfeld "Niederlassung"

Grundsätzlich kann diese Liste beliebig weitergeführt werden. Durch die Festlegung des Anwendungsbereichs über Feldregeln ist der Anwendungsbereich einer Regel sehr flexibel eingrenzbar.

Selbstverständlich kann die Feldregel nicht nur aus einer Bedingung bestehen, sondern es können - wie bei allen Feldregeln - mehrere Bedingungen verknüpft werden, um komplexe Szenarien abzubilden. Siehe dazu auch [Feldregeln](#) (see page 562).

Verwaltung

Neue Einträge in der Entscheidungstabelle können über den Button "Hinzufügen" angelegt werden. Bestehende Einträge können über das Kontextmenü der jeweiligen Zeile bearbeitet oder gelöscht werden.

Tipp

Über den Button "Neue Feldregel" kann eine neue Feldregel angelegt werden, wenn diese benötigt wird. Durch diese Abkürzung muss man nicht zur Verwaltung der Feldregeln wechseln, um eine neue Regel anzulegen.

Wenn Sie eine neue Regel in die Entscheidungstabelle einfügen haben Sie folgende Einstellungsmöglichkeiten:

Einstellung	Beschreibung
Feldregel	Wählen Sie hier die Feldregel aus, auf welche Personen oder Ressourcen zutreffen müssen, damit die Regel für sie Angewandt wird.
Modus	Hier kann eingestellt werden, ob für den gewählten Personenkreis oder die passenden Ressourcen ein Benutzername generiert werden soll oder nicht.
Regel	Mit dieser Einstellung wird die Benutzernamensregel festgelegt, welche verwendet werden soll. Diese Einstellung ist nur sichtbar, wenn in der Einstellung "Modus" die Auswahl "Generieren" getroffen wurde.

Warum nicht generieren?

Die Benutzernamensregeln kommen an mehreren Stellen zum Tragen. Zum einen werden die Benutzernamensregeln von sämtlichen Ressourcen verwendet, welche Benutzerkonten in verschiedenen Systemen darstellen (zum Beispiel Active Directory Benutzerkonten), um einen Benutzernamen bei Zuweisung der Ressourcen zu generieren. Diese Regeln werden jedoch auch bei der Anlage neuer Personen verwendet, um einen Benutzernamen für den Personenstammdatensatz in tenfold zu generieren.

Nicht alle Personen jedoch benötigen einen Benutzernamen. Wenn es sich zum Beispiel um Personen handelt, welche über kein eigenes Benutzerkonto verfügen, dann ist es nicht notwendig, für diese Personen einen Benutzernamen im Stammdatensatz zu generieren. Hierbei könnte es sich zum Beispiel um Personen handeln, welche in Produktionsbetrieben tätig sind und sich dasselbe Benutzerkonto mit anderen Personen teilen. Auch in Krankenhäusern ist es nicht unüblich, dass sich Stationsärzte ein Benutzerkonto teilen und kein persönliches Benutzerkonto erhalten. Ein anderes Beispiel wären Gastbenutzer in Microsoft 365-Umgebungen. Gastbenutzer erhalten keinen Benutzernamen, sondern melden sich mit der E-Mail-Adresse an, mit welcher Sie eingeladen wurden.

Personenarten ohne Benutzernamen

Beim Benutzernamensvorschlag für neue Personen stehen Ihnen nur die Felder "Personenart", "Vorname" und "Nachname" zur Verfügung. Anhand anderer Felder kann initial kein Benutzername vorgeschlagen werden. Legen Sie daher am besten für Personen, welche keine Benutzernamen erhalten, eigene Personenarten an (zum Beispiel: Microsoft 365-Gastbenutzer, Stationsärzte, Produktionsbenutzer) und lassen Sie dort das Feld "Benutzername" weg.

13.7 User Principal Names

Auf dieser Maske lassen sich Regeln definieren, welche zur automatischen Generierung von User Principal Names (UPN) verwendet werden.

Regeln für UPNs
Legen Sie Regeln für die Vorschläge und Generierung von UPN fest.

Regeln

ID	Name	Modus	Anzahl Buchstaben Vorname	Anzahl Buchstaben Nachname	Ressourcen
Default		Konfiguration	Alle	Alle	Alle Ressourcen

Entscheidungstabelle
Sie können die Reihenfolge mittels Drag-and-drop verändern.

ID	Feldregel	Benutzernamen-Regel
Everyone		Default

Sie gelangen auf diese Maske über das Menü *Provisioning > Regelwerke > User Principal Names*.

Benötigte Berechtigung

Für den Zugriff auf diese Maske wird die tenfold-Berechtigung "Manage UPN Rules" (8095) benötigt.

13.7.1 Allgemeines

Zusätzlich zum Anmeldenamen (sAMAccountName) haben Benutzer in Microsoft-Systemen auch einen User Principal Name. Dieser existiert seit Windows 2000 und kann ebenso zur Anmeldung genutzt werden. User Principal Names haben dasselbe Format wie E-Mailadressen, werden jedoch separat gehandhabt. Oftmals ist der interne Domänenname ein anderer als der E-Mail-Adresszusatz. Zum Beispiel max.mustermann@mycompany.local im Gegensatz zu max.mustermann@my-company.com.

Microsoft 365

Microsoft empfiehlt, bei der Verwendung der Microsoft 365 Plattform, die User Principal Names und E-Mail-Adressen gleich zu halten.

Im Gegensatz zu den Benutzernamen kann bei der Anmeldung mit dem User Principal Name die Domäne nicht weggelassen werden. Für die Anmeldung an einer Domäne kann sowohl der Benutzername als auch der User Principal Name verwendet werden. Microsoft 365 erlaubt jedoch nur die Anmeldung über den User Principal Name. Verschiedene Legacy-Systeme wiederum erwarten oftmals die Anmeldung nur über den Benutzernamen. Es ist nicht notwendig, dass die Benutzernamensanteile der beiden übereinstimmen. So kann ein Benutzer zum Beispiel den Anmeldenamen "mmusterm" haben, während der User Principal Name "max.mustermann@mycompany.local" lautet. Dies ist besonders deswegen von Bedeutung, da der Anmeldenamen auf 20 Zeichen beschränkt ist (exklusive Domänenname), während der User Principal Name bis zu 1024 Zeichen (inklusive Domänenname) enthalten darf.

13.7.2 Regeln anlegen oder bearbeiten

Um eine neue Regel anzulegen, klicken Sie im Bereich "Regeln" auf die Schaltfläche "Hinzufügen". Um eine Regel zu bearbeiten, klicken Sie im Aktionsmenü der entsprechenden Regel auf die Aktion "Bearbeiten". Sie können in diesem Aktionsmenü die Regel auch löschen.

Hier kann eine Vielzahl von Einstellungen getroffen werden, welche für die Erzeugung der User Principal Names verantwortlich sind. Diese sind ähnlich zu den Einstellungen der Benutzernamensregeln (siehe [Regeln für Benutzernamen](#)(see page 585)), unterscheiden sich jedoch in manchen Punkten. Die Einstellungen sind wie folgt:

Wo sind die Einstellungen?

Das Erscheinen vieler Einstellungen ist abhängig von der Auswahl anderer Einstellungen. Zum Beispiel erscheint der ganze Bereich "Konfiguration" nur dann, wenn für die Einstellung "Modus" der Wert "Konfiguration" gewählt wurde.

Einstellung	Beschreibung
Bereich "Allgemein"	
Name	Der Anzeigename, welcher innerhalb von tenfold zur Darstellung verwendet wird.
Modus	<p>Legt fest, wie der User Principal Name generiert wird. Sie haben die Möglichkeit, die Erzeugung durch ein Regelwerk zu bestimmen oder durch ein Code Snippet. Verwenden Sie Code Snippets nur dann, wenn die Möglichkeiten der Regeln nicht ausreichend. Im Falle von Code Snippets können zwei unterschiedliche Einstellungen verwendet werden:</p> <ul style="list-style-type: none"> • Verfügbarkeitsprüfung durch Snippet: Das Snippet wird nur einmal aufgerufen und muss selbst die Fremdsysteme auf die Verfügbarkeit des User Principal Names prüfen. Sollte der User Principal Name belegt sein, muss das Snippet selbst Eskalationsschemen anwenden. • Verfügbarkeitsprüfung durch tenfold: Das Snippet wird gegebenenfalls mehrfach aufgerufen. Das Snippet muss nur einen gültigen User Principal Name liefern.
Bereich "Aufbereitung"	
Aufbereitung Vorname	Legt fest, ob der Vorname aufbereitet werden soll, bevor er in den User Principal Name eingefügt wird. Der Name kann hierbei belassen werden, es können Sonderzeichen ersetzt werden (z.B. ä zu ae) oder es kann ein Code Snippet zur Aufbereitung verwendet werden.
Aufbereitung Nachname	Legt fest, ob der Nachname aufbereitet werden soll, bevor er in den User Principal Name eingefügt wird. Der Name kann hierbei belassen werden, es können Sonderzeichen ersetzt werden (z.B. ä zu ae) oder es kann ein Code Snippet zur Aufbereitung verwendet werden.
Schreibweise	<p>Legt die Groß-/Kleinschreibung des User Principal Names fest. Folgende Einstellungen sind vorgesehen:</p> <ul style="list-style-type: none"> • Belassen: Lässt die bestehende Groß-/Kleinschreibung bestehen. (Max.Mustermann@My-Company.local) • Kleinbuchstaben: Wandelt alle Zeichen in Kleinbuchstaben um. (max.mustermann@my-company.local) • Großbuchstaben: Wandelt alle Zeichen in Großbuchstaben um. (MAX.MUSTERMANN@MY-COMPANY.LOCAL) • Code Snippet: Wendet ein Code Snippet an, um die Schreibweise zu bestimmen.

Bereich "Betroffene Ressourcen"	
Modus	Legt fest, ob alle verantwortlichen Ressourcen nach der Verfügbarkeit des UPN überprüft werden sollen oder nur bestimmte.
Ressourcen	Sollte in der vorigen Einstellung "Bestimmte Ressourcen" gewählt worden sein, können hier die zu prüfenden Ressourcen ausgewählt werden. Dies ist dann von Vorteil, wenn zum Beispiel mehrere unabhängige Domänen in Verwendung sind und eine Prüfung aller Domänen eine Verschwendung von Performance darstellen würde. Zur Auswahl stehen hier nur Ressourcen, die Konten in Fremdsystemen repräsentieren (z.B. Active Directory, SAP).
Bereich "Konfiguration"	
Bestandteilen-Modus	Hier kann gewählt werden, ob die Bestandteile Vor-/Nachname oder der Benutzername in der folgenden Auswahl vorhanden sind.
Bestandteile	Hier kann definiert werden, welche Bestandteile für den UPN herangezogen werden und gegebenenfalls auch in welcher Reihenfolge.
Präfix	Ein Präfix, welches vor den Namensteil angefügt wird. Damit können zum Beispiel Admin-Kennungen wie adm.mmuster erzeugt werden.
Vorname	Wählt aus, ob der gesamte Vorname verwendet werden soll oder nur eine bestimmte Anzahl an Zeichen (maximal).
Anzahl	Die Anzahl an Zeichen des Vornamens, welche (maximal) verwendet wird.
Vorname-Teil erhöhen	Mit dieser Einstellung kann bestimmt werden, ob, bei Einschränkung des Vor- und Nachnamens auf eine bestimmte Anzahl von Zeichen, der Vornamensteil verlängert werden darf, wenn der Nachname kürzer ist als erlaubt. Beispiel: Für Vor- und Nachnamen sind jeweils 5 Zeichen erlaubt, was eine Gesamtlänge von 10 Zeichen ergibt. Für eine Person namens <i>Alt, Hubertus</i> könnte dann der Name <i>huberal</i> t entstehen, welcher mit 8 Zeichen kürzer ist als erlaubt. Bei aktivierter Einstellung würde der Name auf <i>hubertualt</i> erweitert werden, um auf die vollen 10 Zeichen zu kommen.
Trennzeichen	Gibt an, welches Trennzeichen zwischen den Vor- und Nachnamensteilen eingefügt wird. Sie können dieses Feld leer lassen, um die beiden Teile direkt zusammenzuhängen. Achtung: Das Trennzeichen wird nur zwischen Vor- und Nachnamen eingefügt. Möchten Sie zwischen Präfix, Suffix und den Namen ein Trennzeichen, so muss dieses im Präfix oder Suffix enthalten sein.
Nachname	Wählt aus, ob der gesamte Nachname verwendet werden soll oder nur eine bestimmte Anzahl an Zeichen (maximal).
Anzahl	Die Anzahl an Zeichen des Nachnamens, welche verwendet wird.

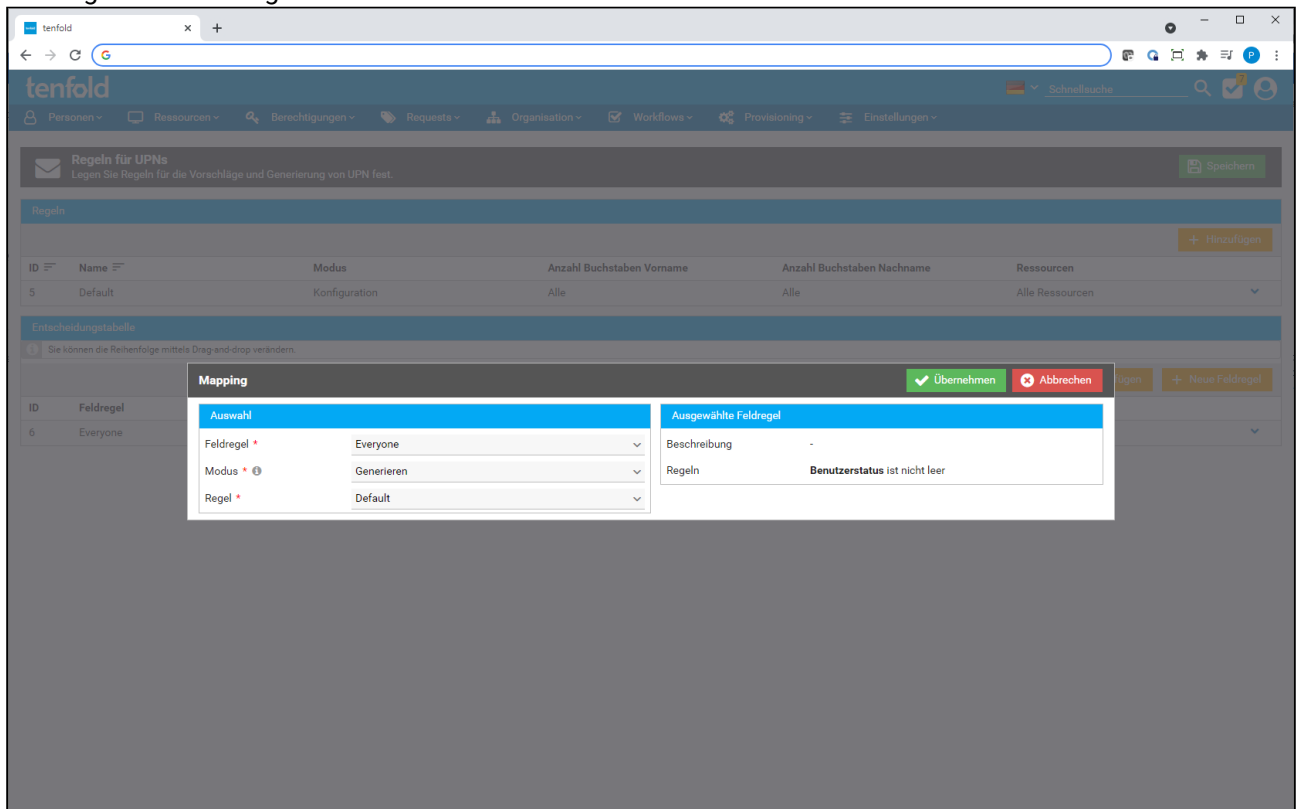
Nachname-Teil erhöhen	Mit dieser Einstellung kann bestimmt werden, ob, bei Einschränkung des Vor- und Nachnamens auf eine bestimmte Anzahl von Zeichen, der Nachname verlängert werden darf, wenn der Vorname kürzer ist als erlaubt. Beispiel: Für Vor- und Nachnamen sind jeweils 5 Zeichen erlaubt, was eine Gesamtlänge von 10 Zeichen ergibt. Für eine Person namens <i>Mustermann, Max</i> könnte dann der Name <i>maxmuste</i> entstehen, welcher mit 8 Zeichen kürzer ist als erlaubt. Bei aktivierter Einstellung würde der Name auf <i>maxmusterm</i> erweitert werden, um auf die vollen 10 Zeichen zu kommen.
Maximale Länge-Modus	Manchmal ist es nicht erwünscht, trotz der Einstellungen "Ganzer Name" für Vor- und Nachnamen, so lange UPNs zu erzeugen. Um dies zu verhindern, kann eine maximale Länge des zu erzeugenden UPN erzwungen werden. Wählen Sie hierfür in dieser Einstellung die Option "Benutzerdefiniert". Mit der Option "Unbegrenzt" werden UPNs beliebiger Länge erzeugt.
Abkürzungsmodus	Legt fest, ob zuerst Zeichen des Vornamens oder des Nachnamens entfernt werden sollen, um einen UPN auf die maximal erlaubte Anzahl von Zeichen zu kürzen.
Maximale Länge	Legt eine Anzahl an Zeichen fest, welche ein gewünschter UPN maximal haben darf.
1. Eskalationsschema	Wählt aus, wie verfahren werden soll, wenn der erzeugte UPN bereits in Verwendung ist. Die Auswahlmöglichkeiten sind: <ul style="list-style-type: none"> • Laufende Nummer: Hängt eine laufende Nummer, beginnend mit 1, an den Namensteil. Diese wird solange erhöht, bis ein freier UPN gefunden wurde. • Weiterer Buchstabe Vorname/Nachname: Kann gewählt werden, um ein weiteres Zeichen des Vor-/Nachnamens zu verwenden (nur für bestimmte Zeichenzahl bei Vor- oder Nachnamen). • Buchstabe Vorname/Nachname entfernen: Es wird ein Buchstabe des Vornamens/Nachnamens entfernt (nur für "Ganzer Name"), bis der Name leer ist. • Buchstabe Vorname bis auf den letzten entfernen: Es wird ein Buchstabe des Vornamens/Nachnamens entfernt, bis nur noch ein Buchstabe des Namens übriggeblieben ist (nur für "Ganzer Name").
2. Eskalationsschema	Sollte im ersten Eskalationsschema die Erweiterung eines Namensteils ausgewählt worden sein, so kann mit dieser Einstellung ausgewählt werden, wie verfahren werden soll, wenn der gewählte Namensteil keine weiteren Buchstaben mehr hat, mit denen ein freier UPN erzeugt werden kann.
3. Eskalationsschema	Ein weiteres Eskalationsschema, analog zu "2. Eskalationsschema". Dieses Schema ist nur verfügbar, wenn bei Vor- oder Nachname die Option "Ganzer Name" ausgewählt wurde.

Suffix	Legt ein Suffix fest, welches nach den Namensbestandteilen angefügt wird, aber noch vor dem @ des UPN-Suffixes. Damit können Admin-Kennungen erzeugt werden, wie zum Beispiel <i>mmuster-adm</i> .
Maximale Länge von (X) Zeichen darf überschritten werden	Diese Einstellung bewirkt, dass der UPN nicht über die maximal denkbare Größe (aufgrund der Einstellungen, die hinterlegt sind) anwachsen darf. Stattdessen wird der UPN auf Kosten bestimmter Bestandteile gekürzt. Beispiel: Wird das Eskalationsschema "Laufende Nummer" genutzt, und wurde für den UPN <i>mmusterm@mycompany.local</i> ein Duplikat festgestellt, so würde, sofern diese Option nicht gesetzt ist, nach der Eskalation der UPN <i>mmusterm1@mycompany.local</i> generiert werden. Wird die Option allerdings gesetzt, sodass die maximale Länge von 8 Zeichen nicht überschritten werden darf, so wird der letzte Bestandteil (in diesem Fall der Nachname) gekürzt und der UPN <i>mmuster1@mycompany.local</i> generiert.
Bereich "Code Snippet"	
Code Snippet	Das Code Snippet, welches aufgerufen wird, um den UPN zu erzeugen. Dieses Snippet sollte, anhand der Personendaten, den Benutzernamensteil des UPN erzeugen (alles vor dem @). Wenn die Verfügbarkeitsprüfung durch das Snippet übernommen wird, muss das Snippet selbst prüfen, ob der generierte UPN vorhanden ist und, wenn nicht, Eskalationsschemen anwenden. Bei der Prüfung durch tenfold wird das Snippet mit einer Historie bereits geprüfter UPNs öfter aufgerufen und muss, anhand der Historie, Eskalationsschemen anwenden.
Bereich "UPN-Suffix"	
Modus	Diese Einstellung bestimmt, ob für die Erzeugung des UPN-Suffixes immer ein fixer Wert herangezogen wird oder ob eine Entscheidungstabelle verwendet wird.
Wert	Legt den Wert fest, welcher für den Modus "Fixer Wert" als UPN-Suffix erzeugt wird. Damit erhalten alle Benutzer immer denselben UPN-Suffix. Achtung: Das @ wird von tenfold automatisch eingefügt und darf im Wert NICHT enthalten sein.
Entscheidungstabelle	Erstellt eine Entscheidungstabelle zur dynamischen Auswahl eines UPN-Suffixes anhand von Feldregeln. In jeder Zeile wird eine Feldregel und ein Wert erwartet. Wenn tenfold dann einen UPN erzeugt, so wendet er die Feldregeln in der angegebenen Reihenfolge an und liefert das Suffix der ersten Zeile, in welcher die Feldregel zutrifft. Achtung: Das @ wird von tenfold automatisch eingefügt und darf im Wert NICHT enthalten sein.

13.7.3 Verwendung der Regeln festlegen

Um festzulegen, welche Regel in welchem Fall verwendet wird, muss im Bereich "Entscheidungstabelle" eine Tabelle angelegt werden. In dieser Tabelle befinden sich pro Zeile eine Feldregel und eine UPN-Regel.

Klicken Sie auf die Schaltfläche "Hinzufügen", um eine neue Zeile in die Tabelle einzufügen. Wählen Sie im daraufhin erscheinenden Dialog die passende Feldregel sowie einen Modus und eine UPN-Regel aus und bestätigen Sie Ihre Eingabe durch Klick auf "Übernehmen".



Für den Modus stehen Ihnen folgende Auswahlmöglichkeiten zur Verfügung:

Modus	Beschreibung
Generieren	Ein Benutzername wird nach der ausgewählten Regel generiert.
Nicht generieren	Es wird kein Benutzername für Personen generiert, welche auf diese Regel zutreffen. Es kann keine Benutzernamensregel ausgewählt werden.

Warum nicht generieren?

Manchmal kann es erforderlich sein, für bestimmte Personengruppen UPNs händisch zu vergeben. Wählen Sie in diesem Fall den Modus "Nicht generieren" und lassen die Anwender den UPN entweder in der Maske "Person bearbeiten" oder durch interaktive Aktivitäten eintragen.

Sollten Sie keine passende Feldregel definiert haben, können Sie über die Schaltfläche "Neue Feldregel" direkt auf die Maske der Feldregeln springen, um dort eine neue Feldregel anzulegen (siehe [Feldregeln](#)(see page 562)). Sobald Sie diese gespeichert haben (oder abbrechen), gelangen Sie wieder auf diese Maske zurück.

Sie können bestehende Zeilen durch einen Klick auf die Aktion "Bearbeiten" im Aktionsmenü bearbeiten oder durch die Aktion "Löschen" aus der Tabelle entfernen.

Wenn tenfold einen UPN mittels Regeln erzeugen soll, wird diese Tabelle in der definierten Reihenfolge ausgewertet. Die UPN-Regel der ersten Zeile, welche eine auf die Person passende Feldregel liefert, wird

angewendet. Wenn keine passende Zeile gefunden wird, so wird der Request, welcher den UPN angefordert hat, fehlschlagen.

Eine einzelne Regel

Diese Entscheidungstabelle ist auch dann notwendig, wenn Sie nur eine einzelne UPN-Regel definiert haben. Fügen Sie in diesem Fall eine Zeile mit der Feldregel "Everyone" und der von Ihnen definierten UPN-Regel hinzu.

13.7.4 Feldmapping oder Regel

Standardmäßig ist tenfold so konfiguriert, dass im Feldmapping für das Active Directory (siehe [Feldmappings](#)(see page 556)) eingestellt ist, dass das AD-Attribut "userPrincipalName" mit einem Standardsnippet "[Username]@[Domain UPN-Suffix]" befüllt wird. Dies bedeutet, dass die auf dieser Maske konfigurierten Regeln zunächst gar nicht verwendet werden.

Um diese Regeln zu aktivieren, müssen Sie zunächst, in der Konfiguration des Active Directory User Lifecycle Plugins, die Einstellung "User Principal Name" im Reiter "Benutzer anlegen" von "Mittels Feldmapping setzen" auf "Von UPN-Regel generieren lassen" ändern. Näheres finden Sie unter [Active Directory User Lifecycle](#)(see page 665).

Update

Die Einstellungen für den User Principal Name sind verfügbar ab der Version 7.1 des Active Directory User Lifecycle Plugins. Eventuell müssen Sie daher erst das Plugin updaten, bevor Sie diese Regeln verwenden können.

13.8 E-Mail-Adressen

Wie Benutzernamen und User Principal Names auch, kann tenfold E-Mail-Adressen für Sie generieren. Analog zu Benutzernamen und UPNs können Sie auch für E-Mail-Adressen Regelwerke zur Generierung erstellen.