tenfold

Administrationshandbuch

Version 16.1.8

1 Table of Contents

2 Verwaltung

2.1 Berechtigungen

2.1.1 Berechtigungen

Berechtigungen gewähren einem Benutzer Zugang zu verschiedenen Bereichen von tenfold. tenfold unterscheidet dabei zwei Arten von Berechtigungen: Vordefinierte Berechtigungen und benutzerdefinierte Berechtigungen.

Vordefinierte Berechtigungen sind bereits bei der Installation von tenfold im System vorhanden und können nicht gelöscht werden. Sie haben eine bestimmte Bedeutung für die Applikation und gewähren dem Benutzer Zugriff auf diverse Funktionen der Anwendung.

Benutzerdefinierte Berechtigungen können von Benutzern angelegt und auch wieder gelöscht werden. Sie haben für die Anwendung zu Beginn keine Bedeutung, können aber wie vordefinierte Berechtigungen auch für gewisse Aktionen konfiguriert werden. Beispielsweise lassen sich bei Genehmigungsworkflows für die einzelnen Genehmigungsschritte Berechtigungen festlegen, die ein Benutzer benötigt um einen Request in diesem Schritt bestätigen zu können.

An folgenden Stellen lassen sich Berechtigungen hinterlegen, die für diverse Aktion benötigt werden:

Bereich	Aktionen	Menü
Personenarten	• Neuanlage von Personen dieser Art • Bearbeiten von Personen deser Art • Anfragen von Services für Personen dieser Art • Anzeigen von Services von Personen dieser Art • Anfragen von Gruppen für Personen dieser Art • Anzeigen von Gruppen von Personen dieser Art • Anfragen von Verzeichnisberechtigungen für Personen dieser Art • Anzeigen von Verzeichnisberechtigungen von Personen dieser Art	Personen / Stammdaten / Personenarten

Personenfelder	• Anzeigen des Feldes • Bearbeiten des Feldes • Erforderlichkeit eines Feldes unterbinden	Personen / Stammdaten / Personenarten
Genehmigungsworkflows	• Genehmigen von Requests	Requests / Genehmigungsworkflows
HTTP Interfaces	• Aufrufen der Schnittstelle per HTTP	Administration / Schnittstellen / HTTP Schnittstellen
Freigaben	• Bearbeiten der Verzeichnisberechtigungen • Anzeige der Freigabe • Anlegen/Umbenennen/Löschen von Verzeichnissen	Windows / Domänen -> Domäne Bearbeiten / Freigaben-Tab

2.1.2 Rollen

Rollen sind eine Zusammenfassung von Berechtigungen, die Benutzern zugeordnet werden können. In tenfold werden Berechtigungen ausschließlich über Rollen zugeordnet und können einem Benutzer nicht direkt zugewiesen werden.

Ein Benutzer kann mehrere Rollen besitzen und jede Rolle kann ihm für eine, mehrere oder alle Abteilungen zugeordnet werden. Ein Benutzer erhält hierbei die Summe aller Berechtigungen für alle Abteilungen, für die ihm Rollen zugeordnet wurden. Das bedeutet, sollte ein Benutzer eine Berechtigung aus einer Rolle erhalten, die ihm für alle Abteilungen zugeordnet wurde und dieselbe Berechtigung aus einer Rolle, die ihm nur für eine Abteilung zugeordnet wurde, so erhält er die Berechtigung für alle Abteilungen.

Vordefinierte Berechtigungen haben hierbei einen Gültigkeitsbereich (siehe Abschnitt "Vordefinierte Berechtigungen"). Berechtigungen mit dem Gültigkeitsbereich "System" treffen keinerlei Unterscheidung zwischen Abteilungen. Hierbei handelt es sich um Berechtigungen, die einem Benutzer zum Beispiel Zugang zu gewissen Stammdatenschirmen gewähren. Es ist hierbei nicht relevant, ob ein Benutzer diese Berechtigung aus Rollen für bestimmte Abteilungen oder für alle Abteilungen erhält.

2.1.3 Definition von Berechtigungen

Die Wartung der Berechtigungen erhalten Sie über den Menüpunkt Administration > ISM-Berechtigungen > Berechtigungen.

Wenn Sie diesen Menüpunkt anwählen, erhalten Sie zunächst eine Liste aller definierten Berechtigungen.

Befindet sich in der Spalte "Benutzerdefiniert" ein , können Sie diese Berechtigung löschen, sofern sie an keiner Stelle verwendet wird. Andernfalls können Sie die Berechtigung nur bearbeiten, um ihr einen neuen Namen zu geben. Neue Berechtigungen können Sie mit dem Icon anlegen. Die Aktionen für Bearbeiten und Löschen befinden sich im Aktionsmenü der jeweiligen Berechtigung.

2.1.4 Definition von Rollen

Um zur Übersicht aller Rollen zu gelangen wählen Sie den Menüpunkt Administration > ISM-Berechtigungen > Rollen.

Wie bei den Berechtigungen, legen Sie neue Rollen mit dem Icon an und finden die Aktionen zum Bearbeiten und Löschen der jeweiligen Rolle im Aktionsmenü in der letzten Spalte.

Im Feld "Name" können Sie der Rolle einen Namen zuweisen. Das Feld "Beschreibung" dient ausschließlich informativen Zwecken und wird nur in der Übersicht der Rollen angezeigt. Schließlich können Sie im Feld "Berechtigungen" der Rolle alle erforderlichen Berechtigungen zuweisen. Die Benutzer denen diese Rolle zugeordnet ist, erhalten somit automatisch die der Rolle zugewiesenen Berechtigungen. In der Liste "Verfügbar" auf der linken Seite befinden sich alle verfügbaren Berechtigungen, die der Rolle noch nicht zugewiesen wurden und in der "Zugewiesen" Liste auf der rechten Seite befinden sich die Berechtigungen, die bereits in der Rolle vorhanden sind. Um der Rolle Berechtigungen zuzuweisen selektieren Sie die gewünschten Berechtigungen in der linken Liste und klicken auf den Zuweisen Button zwischen den beiden Listen. Um Berechtigungen zu entfernen, wählen Sie die vorhandenen Berechtigungen in der rechten Liste und klicken auf den Entfernen Button.

2.1.5 Zuordnung von Rollen

Sobald Sie eine oder mehrere Rollen definiert haben, können sie Personen zugeordnet werden. Hierfür gibt es zwei Möglichkeiten:

Wenn Sie eine Rolle, wie im vorhergehenden Abschnitt beschrieben, bearbeiten, können Sie auf den Tab "Zuweisungen" wechseln.

Hier sehen Sie zunächst sämtliche Personen, die diese Rolle bereits erhalten haben und die entsprechende Abteilung(en). Um einer neuen Person die Rolle zuzuweisen, wählen Sie die Person und Abteilung aus und klicken auf "Hinzufügen". Um einer Person die Rolle für alle Abteilungen zuzuordnen, lassen Sie das Feld Abteilung leer. Das Feld "Benachrichtigung" kann selektiert werden, um Personen zu kennzeichnen, die bei bestimmten Ereignissen oder Aktionen benachrichtigt werden sollen, wenn sie diese Rolle zugeordnet haben. In der Standardkonfiguration von tenfold werden jedoch keine Benachrichtigungen versendet. Das Einrichten dieser Funktionalität muss mit Ihrem tenfold-Betreuer abgesprochen werden.

Um einer Person eine Rolle zu entziehen, benutzen Sie die Aktion "Löschen", die sich im Aktionsmenü neben der jeweiligen Zuordnung befindet.

Alternativ zu dieser Vorgehensweise können Sie im Menü auch Administration > ISM Berechtigungen > Zuordnungen wählen.

Im Tab "Über Personen" können Sie zuerst Personen nach Abteilung, Vor- und Nachname suchen. Anschließend können Sie über die Aktion "Rollen zuordnen" der gewählten Person Rollen zuordnen.

Sie erhalten zunächst eine Übersicht über die Rollen, die die Person schon besitzt. Mit der Aktion Löschen in der letzten Spalte können Sie den jeweiligen Eintrag aus der Liste entfernen.

Um der Person eine neue Rolle hinzuzufügen, wählen Sie die Rolle aus, wählen "Alle Abteilungen" oder eine bestimmte Abteilung und klicken auf hinzufügen. Auch hier können Sie mit dem Feld "Benachrichtigung" Personen markieren, die Benachrichtigungen erhalten sollen wenn sie diese Rolle zugeordnet bekommen.

Auf dem Tab "Über Rollen" können Sie nach Rollen und Abteilungen suchen. Sie erhalten unterhalb der Filterkriterien eine Übersicht über alle Rollen und Abteilungen, die Ihren Suchkriterien entsprechen. Gelb markierte Zeilen stellen Rollen dar - die Einträge darunter die jeweils zugeordneten Abteilungen. Mit dem Button neben einer Rolle können Sie Zuordnungen für eine Abteilung definieren, für die bislang keine Zuordnungen existieren. Mit dem Icon *Bearbeiten* neben einer Abteilung können Sie neue Zuordnungen für die jeweilige Rolle und Abteilung definieren.

Haben Sie den Button neben einer Rolle gewählt, können Sie an dieser Stelle eine Abteilung wählen und anschließend eine Person wählen und per "Hinzufügen" dieser Person die gewählte Rolle zuordnen. Anschließend können Sie diesen Vorgang für weitere Personen wiederholen. Mit der Icon *Löschen* neben einer Zuordnung können Sie diese wieder entfernen.

Haben Sie den Menüpunkt *Bearbeiten* neben einer Abteilung gewählt, gelangen Sie zu dem selben Schirm, jedoch ist die Abteilung bereits ausgewählt und kann nicht mehr verändert werden.

2.1.6 Vordefinierte Berechtigungen

Folgende Berechtigungen sind in tenfold bereits vordefiniert. Berechtigungen mit einem in der Spalte "Enterprise" haben Auswirkungen auf Funktionen, die ausschließlich in der Enterprise Edition von tenfold verfügbar sind.

Berechtigung	Beschreibung	Menüpunkt	Gültigkeitsbereich	Enterprise
ADS groups administration	Erlaubt das Bearbeiten aller Gruppen unabhängig von deren Berechtigungseinstellung.	Windows / Gruppen	System	
Approval context administration	Erlaubt das Erstellen, Bearbeiten und Löschen von Genehmigungskontexten.	Requests / Genehmigungskontexte	System	✓

Approval workflow administration	Erlaubt das Erstellen, Bearbeiten und Löschen von Genehmigungsworkflows.	Requests / Genehmigungsworkflows	System	✓
Approve expirations	Gestattet es einem Benutzer, das Ablaufdatum von anderen Benutzern zu verlängern.	Meine Aufgaben / Abgelaufene Benutzer	Abteilung	
Assign roles	Gestattet es einem Benutzer anderen Personen Rollen zuzuweisen. Rollen können nur an Personen aus Abteilungen und für Abteilungen vergeben werden für welche der Benutzer diese Berechtigung besitzt.	Administration / ISM-Berechtigungen / Zuordnungen	Abteilung	
Batch service assignment	Erlaubt es dem Benutzer, beim Service Shopping, eine Liste mit Personen hochzuladen für welche der Service bestellt werden soll. Dies ist eine administrative Funktion und benötigt daher keine weiteren Bestellberechtigungen für die Abteilungen der einzelnen Personen.	Services / Services kaufen	System	✓
Budget period administration	Erlaubt die Wartung der Budgetperioden.	Finanzen / Budgetperioden	System	✓
Building administration	Erlaubt die Wartung der Gebäude.	Organisation / Gebäude	System	
Bulk change	Erlaubt die Durchführung von Massenpersonenänderngen.	Personen / Massenänderung	System	
Change Own Picture	Erlaubt es einem Benutzer sein eigenes Benutzerbild zu ändern sofern dies für seinen Personentyp zulässig ist.	Personen / Mich selbst bearbeiten	System	

Change own user	Erlaubt es einem Benutzer seine eigenen Personendaten zu bearbeiten. Sollten für einzelne weitere Berechtigungen benötigt werden, muss der Benutzer auch diese Besitzen um die Felder bearbeiten zu können.	Personen / Mich selbst bearbeiten	System	
Change profile expiration	Erlaubt es einem Benutzer den Vorlagen einer Person ein Ablaufdatum zuzuordnen.	Vorlagenzordnungen	System	✅
Company administration	Erlaubt die Wartung der Unternehmen.	Organisation / Unternehmen	System	
Configuration administration	Erlaubt die Wartung der Systemeinstellungen	Administration / Systemeinstellungen	System	
Cost center administration	Erlaubt die Wartung der Kostenstellen	Organisation / Kostenstellen	System	
Create Ads Groups	Erlaubt das Erstellen neuer Active Directory Gruppen.	Windows / Gruppen	System	
Credentials administration	Erlaubt die Wartung von Zugangsdaten	Administration Zugangsdaten	System	✅
Department administration	Erlaubt die Wartung von Abteilungen	Organisation / Abteilungen	System	
Department data owners	Erlaubt die Wartung der Abteilungsverantwortlichen	Organisation / Abteilungen	System	
Department Group administration	Erlaubt die Wartung der Abteilungsgruppen	Organisation / Abteilungsgruppen	System	
Domain administration	Erlaubt die Wartung der Domänen. In der Essentials Edition ist es nur möglich die Einstellungen der Default-Domäne zu ändern, es können jedoch keine neuen Domänen hinzugefügt werden.	Windows / Domänen	System	

Edit user pictures	Erlaubt es einem Benutzer die Benutzerbilder aller Personen zu ändern, für deren Abteilung er diese Berechtigung besitzt.	Person bearbeiten	Abteilung	
Events in requests	Erlaubt einem Benutzer den Events-Tab in der Requestanzeige einzusehen.	Request anzeigen	Abteilung	
Exec flow in requests	Erlaubt einem Benutzer den EXEC-Flow Tab in der Requestanzeige einzusehen.	Request anzeigen	Abteilung	
Execute Batch Syncs	Erlaubt es dem Benutzer einen Personenabgleich durchzuführen.	Administration / Datenabgleich / Personenabgleich	System	
Export FS report	Erlaubt das Exportieren von Berichten über die Zugriffsberechtigungen von Personen auf Freigaben.	Windows / Freigaben, Person anzeigen, AD Objekt anzeigen	Abteilung	
Find department approvers	Erlaubt es dem Benutzer nach Abteilungsverantwortlichen zu suchen.	Personen / Abteilungsverantwortliche	System	
FS Rights administration	Erlaubt die Wartung von Berechtigungssätzen.	Windows / Berechtigungssätze	System	
Global events	Erlaubt Zugriff auf das Ereignis-Log.	Requests / Ereignisse	System	
Http interface administration	Erlaubt die Wartung der HTTP Schnittstellen	Administration / Schnittstellen / HTTP Schnittstellen	System	✅
Identity type administration	Erlaubt die Wartung der Personenarten.	Personen / Stammdaten / Personenarten	System	✅
Job amination	Erlaubt die Wartung der Jobs. Die volle Wartung der Jobs ist nur in der tenfold Enterprise Edition verfügbar. In der Essentials Edition ist es möglich, die Ausführungszeit der vordefinierten Jobs zu ändern.	Administration / Jobs / Verwaltung	System	
Job History administration	Erlaubt Zugriff auf die Job-Historie	Administration / Jobs / Historie	System	✅

Licence Pool Analysis	Erlaubt es dem Benutzer eine Lizenzpoolanalyse durchzuführen	Services / Lizenzpools / Analyse	System	✓
Licence Pool List	Erlaubt die Wartung der Lizenzpools.	Services / Lizenzpools / Verwaltung	System	✓
Login	Gestattet es einem Benutzer tenfold zu verwenden. Ohne diese Berechtigung kann ein Benutzer ungeachtet sämtlicher anderer Berechtigungen die er Besitzt die Anwendung nicht verwenden.	-	System	
Mappings administration	Gewährt Zugang zur Wartung der CMDB- und Kostenstellenzuordnungen	Administration / Datenabgleich / CMDB - Zuordnungen, Administration / Datenabgleich / Kostenstellenzuordnungen	System	
Move to other department	Gestattet einem Benutzer Zugriff zur Seite Abteilungswechsel. Für das verschieben einer Person in eine Abteilung ist es erforderlich diese Berechtigung für die *neue* Abteilung zu besitzen, nicht für die aktuelle.	Personen / Abteilungswechsel	Abteilung	✓
Move to other department suggestion	Erlaubt den Zugriff auf die Liste der automatisch vorgeschlagenen Abteilungswechsel. Es werden alle Personen angezeigt für welche der Benutzer diese Berechtigung für eine der *vorgeschlagenen* Abteilungen besitzt.	Personen / Abteilungswechsel	Abteilung	
Notification administration	Erlaubt die Wartung der E-Mail Vorlagen.	Administration / E-Mails / Vorlagen	System	

NTFS Scans administration	Erlaubt Zugriff auf die NTFS Scan historie.	Windows / NTFS Scans	System	
Office administration	Erlaubt die Wartung der Niederlassungen.	Organisation / Niederlassungen	System	
Organization Unit Group administration	Erlaubt die Wartung der Organisationseinheitsgruppen.	Organisation / Organisationseinheitsgruppen	System	
Organization units administration	Erlaubt die Wartung der Organisationseinheiten.	Organisation / Organisationseinheiten	System	
Password policy administration	Erlaubt die Wartung der Passwortpolicies.	Administration / Policies / Passwort	System	
Person list administration	Erlaubt die Wartung der Personenlisten.	Personen / Stammdaten / Personenlisten	System	
Person title administration	Erlaubt die Wartung von Titeln.	Personen / Stammdaten / Titel	System	
Phone system administration	Erlaubt die Wartung der Telefonanlagen.	Administration / Datenabgleich / Telefonanlagen	System	
Position administration	Erlaubt die Wartung der Positionen	Personen / Stammdaten / Positionen	System	
Privilege administration	Erlaubt es dem Benutzer neue tenfold Berechtigungen zu erstellen, bearbeiten oder zu löschen. Berechtigungen aus dieser Liste können nicht bearbeitet oder gelöscht werden.	Administration / ISM-Berechtigungen / Berechtigungen	System	
Quick search	Erlaubt die Benutzung der Schnellsuche.	-	System	
Request cancel	Erlaubt es einem Benutzer offene Requests abzubrechen. Ein Benutzer kann nur Requests für Personen abbrechen, welche sich in einer Abteilung befinden für welche er diese Berechtigung besitzt.	Requests / Offene Requests, Requests / Alle Requests, Schnellsuche	Abteilung	

Request close	Erlaubt es einem Benutzer offene Requests abzuschließen. Ein Benutzer kann nur Requests für Personen schließen, welche sich in einer Abteilung befinden für Welche er diese Berechtigung besitzt.	Requests / Offene Requests, Requests / Alle Requests, Schnellsuche	Abteilung	
Request log	Erlaubt einem Benutzer den Zugriff auf die Liste der Requests.	Requests / Offene Requests, Requests / Fehlgeschlagene Requests, Requests / Alle Requests	System	
Request reason administration	Erlaubt die Wartung der Request Begründungen.	Requests / Begründungen	Abteilung	✓
Role definition	Erlaubt die Wartung der tenfold-Rollen. Wartung bedeutet erstellen, bearbeiten und löschen von Rollen, jedoch nicht die Zuweisung von Rollen an andere Benutzer.	Administration / ISM-Berechtigungen / Rollen	System	
Script administration	Erlaubt die Wartung der PowerShell- und Unix Shellskripte.	Administration / Scripts	System	✓
Search deleted persons	Erlaubt es einem Benutzer in der Schnellsuche, die Suche nach gelöschten Personen zu aktivieren.	Schnellsuche	System	
Search Persons	Erlaubt es einem Benutzer die Personensuche zu Verwenden	Personen / Personen suchen	System	
Service option administration	Erlaubt die Wartung der Service Optionen.	Services / Verwaltung / Optionen	System	
Service Request Retry	Erlaubt es einem Benutzer fehlgeschlagene Requests zu wiederholen.	Requests / Fehlgeschlagene Requests, Requests / Alle Requests / Schnellsuche	System	

Service shopping	Erlaubt einem Benutzer das Nutzen der Service Shopping Funktion.	Services / Einkaufen	System	✓
Services administration	Erlaubt die Wartung der Services.	Services / Verwaltung / Services	System	✓
Set data owner	Erlaubt es einem Benutzer Personen als Dateneigentümer von Active Directory Gruppen oder Verzeichnissen festzulegen.	Windows / Gruppen, Windows / Freigaben	System	
Template preview	Erlaubt es einem Benutzer die Vorlagenvorschau zu verwenden.	Personen / Vorlagen / Vorschau	System	✓
Templates	Erlaubt die Wartung der Personenvorlagen	Personen / Vorlagen / Verwaltung	Abteilung	✓
User name suggestion	Erlaubt es einem Benutzer die Funktion zum Vorschlagen von Benutzernamen zu verwenden	Personen / Benutzername vorschlagen	System	✓
Value group configuration administration	Erlaubt die Wartung der Nachschlagewerte.	Administration / Nachschlagewerte	System	
Verification policy administration	Erlaubt die Wartung der Verifizierungspolicies.	Administration / Policies / Verifizierung	System	
View assignments	Erlaubt einem Benutzer den Zugang zur Übersichtsseite für Servicezuordnungen. Auf der Seite zur Berechtigungsanalyse können nur Abteilungen ausgewählt werden, für welche der Benutzer diese Berechtigung besitzt.	Services / Zuordnungen, Services / Berechtigungen / Analyse, Schnellsuche	Abteilung	✓
View audit log	Erlaubt einem Benutzer Zugriff auf die Historie von allen Personen die sich in Abteilungen befinden für welche er diese Berechtigung besitzt.	Personen / Personen suchen, Personen / Benutzername vorschlagen, Schnellsuche	Abteilung	

View compliance review	Erlaubt es einem Benutzer den Vorlagenabgleich aller Personen zu sehen, welchen in Abteilungen sind für welche er diese Berechtigung besitzt.	Schnellsuche	Abteilung	✅
View data owners	Gewährt einem Benutzer Zugang zur Übersicht der Dateneigentümer	Windows / Dateneigentümer	System	
View Department	Gewährt lesenden Zugriff auf die Abteilungsstammdaten.	Organisation / Abteilungen	System	
View department cost allocation	Gewährt Zugriff zur Kostenumlage.	Finanzen / Kostenumlage	System	✅
View disabled persons/ services	Erlaubt den Zugriff zur Seite Gelöschte Servicezuordnungen.	Personen / Gelöschte Servicezuordnungen	System	✅
View future requests	Erlaubt es dem Benutzer sich die Liste der Zukünftigen Requests anzusehen.	Requests / Zukünftige Requests	System	✅
View Online Users	Erlaubt einem Benutzer Zugriff auf den Session Manager. ⚠️ Bitte beachten Sie die nachfolgenden Ausführungen im Abschnitt Session Manager (see page 17).	Administration / Session Manager	System	
View Organization Unit	Gewährt lesenden Zugriff auf die Stammdaten der Organisationseinheiten	Organisation / Organisationseinheiten	System	
View own user	Gestattet lesenden Zugriff auf die eigenen Personendaten.		System	
View password reset history	Gewährt Zugriff zur Passwort-Historie.	Requests / Passwort-Historie	System	
View person	Erlaubt es einem Benutzer sich die Daten aller Personen anzeigen zu lassen, welche sich in Abteilungen befinden, für welche er diese Berechtigung besitzt.		Abteilung	
View privilege analysis	Gewährt Zugang zur Berechtigungsanalyse.	Services / Berechtigungen / Analyse	Abteilung	✅

View profile expiration history	Gewährt Zugriff auf die Vorlagenhistorie von Personen.	Vorlagenzordnungen	System	✓
View Service Masterdata	Gewährt lesenden Zugriff auf die Service Stammdaten.	Services / Verwaltung / Services	System	✓
View System Information	Erlaubt es einem Benutzer die tenfold Systeminformation anzuzeigen.	Administration / Systeminformationen	System	
View template alignments	Erlaubt einem Benutzer den Zugriff zum Vorlagenabgleich von Personen welche sich in Abteilungen befinden, für welche er diese Berechtigung besitzt.	Personen / Vorlagen / Abgleich	Abteilung	✓
View template assignments	Erlaubt einem Benutzer den Zugriff auf die Vorlagenzuordnungen von Personen, welche sich in Abteilungen befinden, für welche er diese Berechtigung besitzt.	Personen / Vorlagen / Zuordnungen	Abteilung	✓
Workflow amministration	Erlaubt die Wartung der EXECs.	Administration / EXECs / Verwaltung, Administration / EXECs / Suche	System	✓

2.1.7 Session Manager

Über den Menüpunkt Administration > Session Manager erhalten Sie Zugriff zu einer Liste aller Benutzer, die gerade in tenfold angemeldet sind.

Im Menü in der letzten Spalte jeder Benutzerzeile finden Sie die Aktion "Benutzer anzeigen" und "Session beenden". Mit "Benutzer anzeigen" gelangen Sie auf die Stammdatenseite des Benutzers. Mit "Session beenden" können Sie die aktuelle Sitzung des Benutzers löschen, was dazu führt, dass er bei seinem nächsten Zugriff auf tenfold neu angemeldet wird.

Über der Tabelle der angemeldeten Personen befindet sich das Feld "Sitzung ändern". In diesem Feld können Sie eine beliebige Person angeben, um anschließend mit dem Button *Sitzung ändern* Ihre aktuelle Sitzung zu schließen und sich als die ausgewählte Person neu anzumelden. Dieser Vorgang erfordert niemals das Passwort des ausgewählten Benutzers.

> Diese Funktion erlaubt es, jede Person im System zu personifizieren, selbst Personen mit höheren Berechtigungen als die des aktuellen Benutzers. Rollen mit der Berechtigung *View Online Users* sollten daher niemals leichtfertig vergeben werden.

Mithilfe dieser Funktion können Sie tenfold aus Sicht eines bestimmten Benutzers betrachten, um zu prüfen, welche Aktionen dieser Benutzer vornehmen kann und welche Daten er sieht. Diese Funktion ist für jene Benutzer nützlich, die Rollen und Berechtigungen verwalten. Mit Hilfe davon kann festgestellt werden, ob der jeweilige Benutzer ausschließlich die Rechte besitzt, die ihm zustehen.

2.2 Jobs

2.2.1 Allgemeines

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

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

Jeder Job kann auf drei Arten gestartet werden:

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

2.2.2 Verwaltung

> **Benötigte Berechtigung**
>
> Um die Job-Verwaltung durchzuführen, wird die Systemberechtigung "Job Aministration" (8013) benötigt.

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

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

Editionen

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

Spezielle Jobs

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

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

Liste der Jobs

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

- Name: die Bezeichnung des Jobs
- Typ: Gibt an, ob es sich um einen zeitgesteuerten oder einen dateigesteuerten Job handelt
- Cron-Auslöser: Gibt im Falle eines zeitgesteuerten Jobs den hinterlegten Cron-Auslöser an (für dateigesteuerte Jobs ist dieser Wert immer leer)
- Dateiauslöser: Gibt im Falle eines dateigesteuerten Jobs den hinterlegten lokalen oder UNC-Pfad für die zu überwachende Datei an (für zeitgesteuerte Jobs ist dieser Wert immer leer)
- Nächste Durchführung: Gibt im Falle von zeitgesteuerten Jobs den nächsten planmäßigen Durchführungszeitpunkt an (für dateigesteuerte Jobs ist dieser Wert immer leer)

Job-Einstellungen bearbeiten

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

Es können anschließend folgende Einstellungen getroffen werden:

Einstellung	Beschreibung	Beispielwert
Name	Legt die Bezeichnung des Jobs fest. Diese dient lediglich der Darstellung innerhalb von tenfold.	My new job

Typ	Bei der Anlage eines Job wird festgelegt, ob es sich um einen zeitgesteuerten (Cron-Auslöser) oder dateigesteuerten (Dateiauslöser) Job handelt. Diese Einstellung kann im Nachhinein nicht mehr geändert werden, und wird lediglich zur Information angezeigt.	
Cron-Auslöser (nur bei zeitgesteuerten Jobs)	Hier wird im Crom-Format festgelegt, zu welchen Zeitpunkten der Jobs gestartet werden soll. Zur Erläuterung des Cron-Formats siehe http://www.quartz-scheduler.org/documentation/quartz-2.x/tutorials/crontrigger.html	0 0 22 ? * * (bedeutet jeden Tag um 22:00)
Dateiauslöser (nur bei dateigesteuerten Jobs)	Es wird der Pfad zur Datei festgelegt, welche überwacht werden soll. Es werden sowohl lokale Dateien auf dem tenfold Server, als auch Dateien auf anderen Rechner (via UNC-Pfad) unterstützt.	C:/mydir/myfile.csv \\srv1-fs\mydir\myfile.csv
EXEC	Legt fest, welcher EXEC für die Bearbeitung des Jobs vorgesehen ist.	
Aktiv	Hier kann festgelegt werden, ob der Job aktiv ist oder nicht. Wird ein Job deaktiviert, so wird der entsprechende EXEC nicht ausgeführt, auch wenn der Cron- oder Dateiauslöser auslöst.	

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

Cron-Auslöser Beispiele

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

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

0 15 10 ? * MON-FRI	Der Job startet Montag bis Freitag jeweils um 10:15 Uhr

Job löschen

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

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

Job ausführen

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

Ausführung abbrechen

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

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

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

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

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

2.2.3 Historie

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

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

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

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

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

Für jeden Eintrag werden Informationen angezeigt:

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

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

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

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

Status "Nicht ausgeführt"

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

Detallierte Informationen zu Scans

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

2.3 Organisationsstruktur

Im Menü *Organisation* befinden sich mehrere Punkte zur Verwaltung Ihrer Organisationsstruktur innerhalb von tenfold. Mithilfer dieser Struktur können Sie in tenfold steuern wie Benutzer angelegt werden sollen, können die Berechtigungen der Benutzer innerhalb von tenfold Einschränken, etc. Im weiteren ist die Organisationsstruktur im wesentlichen dafür gedacht, Personen für eine automatische Zuordnung von Profilen zu identifizieren (Siehe Profile). Im Folgenden werden die einzelnen Einstellungen zur Organisationsstruktur genauer beschrieben.

2.3.1 Abteilungen

Abteilungen bilden die Grundlagen für das Berechtigungskonzept von tenfold (siehe Berechtigungen (see page 5)). In tenfold kann eine Person entsprechende Berechtigungen immer entweder für Alle oder für bestimmte Abteilungen besitzen. Dadurch lässt sich der Personenkreis einschränken, für welche ein Benutzer von tenfold Anfragen stellen und/oder Genehmigen kann.

Abteilungen

Organisation > Abteilungen.

Eine Person kann einer Abteilung mittels des Personenfeldes *DEPARTMENT* zugeordnet werden (siehe Personenfelder).

Feld	Beschreibung	Beispielwert
Name	Der Name der Abteilung. In der Standardkonfiguration wird dieses Feld der ausgewählten Abteilung einer Person in das Active Directory Feld *Abteilung* übertragen.	Information Technology

Kurzname	Ein Kürzel für die Abteilungsbezeichnung. In manchen Fällen ist es wünschenswert dieses Feld in das Active Directory zu übertragen, statt dem vollen Namen, ohne dabei auf einen sprechenden Namen in tenfold Verzichten zu wollen.	IT
Typ	Hier kann eine Eingliederung in verschiedene Arten von Abteilungen vorgenommen werden.	Intern, Extern
Beschreibung	Eine Beschreibung der Abteilung zu informativen Zwecken.	
Übergeordnete Abteilung	Hier lässt sich die übergeordnete Abteilung einstellen. Hiermit lassen sich Abteilungshierarchieen erstellen. (Siehe Abteilungshierarchie (see page 26)) Diese ist relevant für die Genehmigung von Requests (siehe Abteilungsverantwortliche (see page 25)).	Information Technology (Dropdown-Auswahl)
Abteilungsgruppe	Hier lässt sich die Abteilung zu einer Gruppe zuordnen. (Siehe Abteilungsgruppen (see page 26))	Technology
Region	Hier lässt sich die Region einer Abteilung einstellen. Von der Region einer Person hängt ab, wieviel Services für diese Person kosten.	EU
Standardniederlassung	Hier kann eine Standardniederlassung für die Abteilung eingestellt werden. Diese kann zum Beispiel verwendet werden um in Synchronisationsprozessen von Fremdsystemen welche nur Abteilungen kennen eine Niederlassung für eine Person festzulegen.	Büro Seidengasse
AD-Container	Ein Active Directory Container welcher zum Beispiel benutzt werden kann um Personen anhand ihrer Abteilung in das Active Directory einzugliedern. In der Standardkonfiguration wird dieses Feld jedoch nicht Berücksichtigt sondern nur die Einstellung *Container für Benutzer* der Domäne.	OU=IT,OU=USR,OU=CERTEX,OU=AT

Berechnungsmodus	Die Art der Berechnung welche für die Kostenumlage einer Person dieser Abteilung herangezogen wird. In der Standardkonfiguration sind folgende 3 Berechnungsvarianten vorhanden: • Keine Verrechnung: Die Kosten einer Person sind immer 0. • Normale Verrechnung: Die Kosten einer Person ist die Summe aller Kosten ihrer Services • Maximum Verrechnung: Die Kosten einer Person sind die Kosten des teuersten Services jener Person.	Normale Verrechnung
Parameter	Hier können Benutzerdefinierte Parameter hinzugefügt werden, welche in Anpassungen herangezogen werden können.	

Abteilungstypen

Für Abteilungstypen gibt es in der aktuellen Version keine Wartungsmaske. Diese werden manuell in der tenfold-Datenbank angelegt. Bitte wenden Sie sich an Ihren Betreuer.

Abteilungsverantwortliche

Um die Verantwortlichen einer Abteilung zu bearbeiten rufen Sie den Menüpunkt *Organisation > Abteilungen* auf und wählen im Anschluss, im Aktionsmenü der entsprechenden Abteilung, den Menüpunkt *Verantwortliche*.

Abteilungsverantwortliche kommen in Genehmigungsworkflows zum tragen. Sollte in einem Genehmigungsworkflow die Berechtigung *Dateneigentümer* ausgewählt sein und es sich bei einem Request um einen Personenänderungsrequest handeln, so kann dieser Schritt von jeder Person genehmigt werden, welcher ein Abteilungsverantwortlicher für die Abteilung der betroffenen Person ist. Sollte für die entsprechende Abteilung kein Verantwortlicher eingetragen sein, so wird in der übergeordneten Abteilung nach einem Verantwortlichen gesucht, so lange bis jemand gefunden wurde. Sollte in der gesamten Hierarchie kein Verantwortlicher gefunden worden sein, so kann dieser Schritt von einer Person mit der Berechtigung *Default Approve Privilege* genehmigt werden.

Vererbung von Abteilungsverantwortlichen

Eine Vererbung von Abteilungsverantwortlichen wird in der aktuellen Version nicht unterstützt. Sobald in einer Abteilung Verantwortliche gefunden wurden, werden Verantwortliche von übergeordneten Abteilungen nicht mehr befragt. Sie müssen daher

Personen in untergeordneten Abteilungen erneut hinzufügen, wenn Sie möchten, dass eine Person auch in untergeordneten Abteilungen genehmigen darf.

Um einen Verantwortlichen hinzuzufügen, wählen sie im Feld *Person* eine Person aus, und klicken auf *Hinzufügen.* Wenn Sie das Feld *Benachrichtigung* aktiviert haben, so wird der entsprechenden Person immer per E-Mail mitgeteilt, wenn es entsprechende Requests für sie zu genehmigen gibt. Wurde dieses Feld nicht aktiviert, so erhält die Person keine Benachrichtigung per E-Mail. Dies kann nützlich sein, wenn Sie eine Person in sehr vielen Abteilungen als Verantwortlichen eingetragen haben, diese Person jedoch zum Beispiel nur als Vertretung agieren und demnach nicht im Normalfall benachrichtigt werden soll. Im Aktionsmenü des jeweiligen Eintrages lassen sich Personen wieder als Verantwortliche entfernen.

Nachträgliches Bearbeiten des Feldes Benachrichtigung

Sollten Sie im Nachhinein das Feld *Benachrichtigung* setzen oder löschen wollen, müssen Sie den Eintrag der entsprechenden Person entfernen und anschließend mit/ohne Benachrichtigung neu hinzufügen.

Abteilungsgruppen

Organisation > Abteilungsgruppen

Abteilungsgruppen sind Gruppierungen von Abteilungen. Eine Abteilung kann dabei immer nur einer einzigen Gruppe angehören. Eine Person gehört daher immer der Abteilungsgruppe der Abteilung an in welcher sie sich befindet. Der Hauptzweck von Abteilungsgruppen besteht darin Profile für mehrere Abteilungen anlegen zu können.

Gruppe von Abteilungen vs. Abteilungsuntergruppen

Abteilungsgruppen befinden sich in der Hierarchie überhalb der Abteilungen. Es handelt sich hierbei *nicht* um Untergruppen von einzelnen Abteilungen.

Feld	Beschreibung	Beispielwert
Name	Der Name der Abteilungsgruppe. Diese Bezeichnung wird in tenfold angezeigt.	Alle Abteilungen
Kurzname	Ein Kürzel für die Abteilungsgruppe.	ALL
Beschreibung	Eine informative Beschreibung.	

Abteilungshierarchie

Organisation > Abteilungshierarchie

Dies ist eine Übersichtsmaske zur Darstellung der Abteilungshierarchie innerhalb Ihrer Organisation. Sie können sich hier in einer Baumstruktur die Gliederung Ihrer Abteilungen anzeigen lassen, sowie sich die einzelnen Verantwortlichen einer jeden Abteilung ansehen. (Siehe Abteilungsverantwortliche (see page 25))

2.3.2 Kostenstellen

Organisation > Kostenstellen

Kostenstellen können Personen über das Personenfeld *COST_CENTER* oder *IT_COST_CENTER* zugeordnet werden (siehe Personenfelder). In der Standardkonfiguration sind diese Einstellungen rein informativ und haben keine besondere Bedeutung für tenfold.

> ⚠ **Bearbeiten von Kostenstellen**
>
> Momentan ist eine Bearbeitung von Kostenstellen mittels eines Schirmes in tenfold nicht vorgesehen. Sie sind gedacht um aus Fremdsystem (z.B. SAP) importiert zu werden. Wenden Sie sich bitte an Ihren Betreuer wenn Sie Kostenstellen aus einem anderen System importieren möchten.

2.3.3 Organisationseinheiten

Organisationseinheiten bieten Ihnen die Möglichkeit Ihre Organisation in verschiedene Bereiche aufzuteilen. Im Gegensatz zu Abteilungen handelt es sich hierbei jedoch nicht um eine Gliederung nach Personalbereichen, sondern um eine Aufteilung innerhalb Ihrer IT-Landschaft.

Organisationseinheiten

Organisation > Organisationseinheiten

Ein Benutzer ist über seine Niederlassung zu einer Organisationseinheit zugehörig. In dieser Organisationseinheit können Einstellungen über seine Domänenzugehörigkeit u.Ä festgelegt werden.

Feld	Beschreibung	Beispielwert
Name	Der Name der Organisationseinheit. Der Name dient lediglich zur Anzeige in tenfold.	Certex
Code	Ein Kürzel, zur Identifizierung der Organisationseinheit. Dieses Feld kann z.B. in Anpassungen verwendet werden um eine Organisationseinheit in Fremdsystemen zu identifizieren.	CER

Beschreibung	Eine Beschreibung der Organisationseinheit. Hier können Sie Informationen zum Zweck der Organisationseinheit hinterlegen.	
Typ	Die Art der Organisationseinheit. Hiermit lassen sich Organisationseinheiten z.B in Physische oder Logische Einheiten untergliedern.	Physical Site
Domäne	Hier legen Sie fest zu welcher Active Directory Domäne ein Benutzer gehört.	certex (Dropdown-Auswahl)
Freigabe für "Eigene Dateien"	Hier kann festgelegt werden wo sich der Ordner befindet in welchem Home-Verzeichnisse für Personen angelegt werden sollen. Ist dieses Feld leer, so wird für einen Benutzer dieser Organisationseinheit kein Home-Verzeichnis angelegt. Ist dieses Feld befüllt wird einem Benutzer ein Home-Verzeichnis angelegt wenn er erstellt wird.	\\fileserver\home
Gruppenabgleich	Hier kann hinterlegt werden ob Mitglieder dieser Organisationseinheit an Active Directory-Gruppen-Abgleichen teilnehmen. Zum Beispiel lässt sich ein Abgleich einrichten, der allen Mitgliedern einer bestimmten Gruppe gewisse Services zuordnet.	Ja/Nein
AD-Container	Hier lässt sich ein Active-Directory Container eintragen in welchem Personen dieser Organisationseinheit abgelegt werden. In der Standardkonfiguration wird nur die Einstellung *Container für Benutzer* der Domäne herangezogen. In Anpassungen kann dieser Wert jedoch herangezogen werden.	OU=USR,OU=CERTEX,OU=AT
Mail-Server	Hier lässt sich Einstellen welcher Mail-Server für die Person zuständig ist.	mail-system.certex.at
Mail-Domain	Hier lässt sich eine E-Mail Domäne festlegen. Diese kann zum Beispiel verwendet werden um einen Vorschlag für die E-Mail-Adresse neuer Personen zu generieren.	certex.at
Mailbox-Store	Hier kann für die Anlage einer Mailbox für eine Person die Datenbank hinterlegt werden in welche Personen dieser Organisationseinheit gespeichert werden sollen.	mailstore1.edb
Externe ID	Hier kann eine alternative ID angegeben werden, welche zur Identifizierung des Mailbox-Stores in Fremdystemen dient.	

Parameter	Hier können Benutzerdefinierte Parameter für eine Organisationseinheit hinterlegt werden, welche in Anpassungen herangezogen werden können.	

Organisationseinheitstypen

Für die Wartung der Organisationseinheitstypen existiert keine eigenständige Wartungsmaske. Die einzelnen Typen werden in den Nachschlagenwerten festgehalten.

Organisationseinheitsgruppen

Organisation > Organisationseinheitsgruppen

Unter einer Organisationseinheitsgruppe können Sie eine oder mehrere Organisationseinheiten zusammenfassen. Der Hauptzweck von Organisationseinheitsgruppen ist es die Örtliche Verfügbarkeit von Services einzuschränken. In jedem Service lassen sich ein oder mehrere Organisationseinheitsgruppen definieren, in welchen der Service verfügbar ist. Damit können nur Personen, welcher in ihrer Hauptniederlassung zu einer Organisationseinheit einer solchen Gruppe gehören, diesen Service bestellen.

Feld	Beschreibung	Beispielwert
Name	Der Name der Gruppe. Dieser wird in tenfold angezeigt.	Alle, Europa, Deutschland
Kurzname	Ein Kürzel für den Namen.	ALL, EU, DE
Organisationseinheiten	Eine Liste aller Organisationseinheiten welche in der Gruppe enthalten sind. Eine Organisationseinheit kann zu mehreren Gruppen gehören.	

Services

Services sind nur in der Enterprise Edition von tenfold enthalten.

2.3.4 Unternehmen & Niederlassungen

Mit diesen Strukturen lassen sich die einzelnen Orte verwalten, welchen Ihre Benutzer ihrer Arbeit nachgehen. Eine Person kann hierbei einer oder mehreren Niederlassungen zugeordnet sein, wobei immer genau eine Niederlassung als seine Hauptniederlassung herangezogen wird. Über diese Hauptniederlassung wird in tenfold die Zugehörigkeit zu den einzelnen Unternehmen sowie zu einer Organisationseinheit hergestellt.

Unternehmen

Organisation > Unternehmen

Bei Unternehmen handelt es sich um Stammdatensätze welche die einzelnen Firmen und/oder Gesellschaften in Ihrer Organisation abbilden. In der Standardkonfiguration dient dies dazu, die Daten in Ihrem Active Directory einheitlich zu halten. Eine Person erhält seine Zugehörigkeit zu einem Unternehmen über seine Hauptniederlassung. Damit vermeiden Sie Doppel- und Fehleingaben im Feld "Firma" und das Feld wird auch automatisch aktualisiert, sollte der Benutzer in eine andere Niederlassung wechseln.

Feld	Beschreibung	Beispielwert
Name	Der Name des Unternehmens. Dieses Feld wird in der Standardkonfiguration in das Active Directory übertragen. Hierbei wird das Unternehmen der Hauptniederlassung einer Person in das Feld "Firma" geschrieben.	certex Information Technology GmbH
Code	Ein Kürzel für das Unternehmen. Hier kann man zum Beispiel Identifizierer für das Unternehmen eintragen welche in Ihrer IT-Landschaft verwendet werden.	CER
Abteilungsverweis	Hier kann eine Abteilung ausgewählt werden. Dieses Feld hat in der Standardkonfiguration keine Auswirkung, kann aber in Anpassungen berücksichtigt werden.	IT (Dropdown-Auswahl)
Übergeordnetes Unternehmen	Sollten die einzelnen Unternehmen in Ihrer Organisation in einer Mutter-Tochter-Beziehung zueinander stehen, so lässt sich hier die Muttergesellschaft eintragen.	certex Information Technology GmbH (Dropdown-Auswahl)

> ⚠ **Niederlassung & Unternehmen**
>
> In den Personenfeldern einer Personenart kann das Feld *COMPANY* hinzugefügt werden, welches die Auswahl eines Unternehmens bei einer Person erlaubt. Es wird dennoch in der Standardkonfiguration immer das Unternehmen der Hauptniederlassung in das Active Directory übertragen.

Niederlassungen

Organisation > Niederlassungen

Bei Niederlassungen handelt es sich um die einzelnen Standorte an welchen die Personen Ihrer Organisation tätig sind. In der Standardkonfiguration werden diese Datensätze dazu verwendet die

Daten in Ihrem Active Directory konsistent zu halten. Damit lassen sich Doppel- und Fehleingaben vermeiden. Personen ein und derselben Niederlassung erhalten hierbei immer dieselbe Adresse in derselben Schreibweise im Active Directory.

Eine Niederlassung kann einer Person über das Personenfeld *OFFICE* zugeordnet werden (siehe Personenfelder).

Feld	Beschreibung	Beispielwert
Name	Der Name der Niederlassung. Dieser wird in das Feld *Büro*, des Active Directory geschrieben.	Wien Seidengasse
Typ	Eine Auswahl des Typs der Niederlassung. In den Einstellungen der Personenarten lässt sich für eine Personenart festlegen, welcher Typus von Niederlassung zulässig ist.	Interne/Externe Niederlassung
Code	Ein Kürzel für die Niederlassung. Hier lässt sich z.B. ein Code eingeben, welcher in Ihrer IT-Landschaft für die Niederlassung verwendet wird.	VIE
Organisationseinheit	Die Organisationseinheit zu welcher die Niederlassung gehört.	Standard
Unternehmen	Das Unternehmen zu welcher die Niederlassung gehört.	certex Information Technology GmbH
Beschreibung	Eine Beschreibung der Niederlassung zu informativen Zwecken.	Dies ist das HQ des Unternehmens.
Telefon	Die Hauptdurchwahl der Niederlassung. Dieses Feld wird nicht zu einer Person in das Active Directory übertragen. In den Personenstammdaten befindet sich hierfür ein eigenes Feld.	+43 (0)1 / 66 50 633
Fax	Die Hauptdurchwahl für das Fax der Niederlassung. Dieses Feld wird nicht zu einer Person in das Active Directory übertragen. In den Personenstammdaten befindet sich hierfür ein eigenes Feld.	+43 (0)1 / 66 50 633
Straße	Die Straße, Hausnummer, etc der Niederlassung. Dieses Feld wird zu einer Person in das Active Directory übertragen.	Seidengasse 9-11, Top 3.4
Stadt	Die Stadt in welcher sich die Niederlassung befindet. Dieses Feld wird zu einer Person in das Active Directory übertragen.	Wien

PLZ	Die Postleitzahl in welcher die Niederlassung zu finden ist. Dieses Feld wird zu einer Person in das Active Directory übertragen.	1070
Bundesland/Kanton	Das Bundesland/der Kanton in welcher/ welchem sich die Niederlassung befindt.	Wien
Land	Das Land in welcher sich die Niederlassung befindet. Dieses Feld wird zu einer Person in das Active Directory übertragen.	Austria
Gebäude	Hier lassen sich einzelne Gebäude zu einer Niederlassung zuordnen, falls es sich bei der Niederlassung zum Beispiel um einen Komplex aus mehreren Gebäuden an derselben Adresse handelt.	Produktionshalle, Verwaltungsgebäude
Parameter	Hier lassen sich mehrere vordefinierte Parameter zu der Niederlassung hinzufügen, welche in den Anpassungen Ihrer Installation verwendet werden können.	

Niederlassungstypen

In der aktuellen Version von tenfold existiert kein Wartungsschirm für die Niederlassungstypen. Diese müssen manuell in der Datenbank gewartet werden. Kontaktieren Sie hierfür bitte Ihren Betreuer.

Gebäude

Organisation > Gebäude

Sollten Sie in einer oder mehrere Ihrer Niederlassungen mehrere Gebäude unter einer Anschrift haben, so können Sie hier die Gebäude definieren, welche sie einzelnen Niederlassungen zuordnen können. In der Standardkonfiguration haben Gebäude keine Funktionen, können jedoch in Anpassungen herangezogen werden.

Feld	Beschreibung	Beispielwert
Name	Der Name des Gebäudes	Hauptgebäude, Produktionshalle
EID	Ein Identifizierer, welcher in Ihrer IT-Landschaft für ein Gebäude verwendet wird.	CER-BLD-1
Code	Ein Kürzel welches für dieses Gebäude verwendet wird.	HQ

2.4 Personenstammdaten

In den Personenstammdaten lassen sich verschiedene Einstellungen treffen die sich darauf auswirken wie tenfold bestimmte Personen behandelt und verwaltet.

2.4.1 Personenarten

Menü > Personen > Stammdaten > Personenarten

Jede Person in tenfold ist immer genau einer Art von Person zugeordnet. Mithilfe dieser Art lassen sich Personen in verschiedene Typen von Person einteilen. Ein Beispiel hierfür wäre eine Einteilung in Interme Mitarbeiter und Externe Mitarbeiter.

Zu einer Personenart werden bestimmte Einstellungen hinterlegt, wie zum Beispiel welche Prozesse zur Anlage oder Bearbeitung herangezogen werden oder auch wer Anfragen zu einer Person dieser Art stellen oder genehmigen darf.

Weiters lässt sich auch bei der automatischen Profilzuordnung (Siehe Profile) nach der Art einer Person filtern.

> **Enterprise-Feature**
>
> Neue Personenarten lassen sich nur in der Enterprise Edition von tenfold hinzufügen. In der Essentials- und Essentials Plus-Edition von tenfold kann nur die Mitgelieferte Standardpersonenart *Mitarbeiter* bearbeitet werden.

In den folgenden Abschnitten folgt eine Übersicht über die Einstellungen welche man bei einer Personenart treffen kann.

Tab: Personenart

Allgemeine Einstellungen

Folgende Einstellungen sind rein deskriptiver Natur und dienen der Anzeige in tenfold.

Feld	Beschreibung	Beispielwert
Name	Der Name der Personenart. Diese wird in tenfold angezeigt	Mitarbeiter, Externer Consultant, Sammelbenutzer
Personen-Icon	Der Name des Icons welches verwendet werden soll.	user, businessman, stockbroker3

Beschreibung	Eine rein informative Beschreibung über den Zweck der Personenart.	

Liste der Icons

Eine Liste der Icons erhalten Sie, mittels der Icon-Aktion in der Titelleiste der Seite.

Execs

Folgende Einstellungen steuern die Prozesse welche durchgeführt werden, sobald eine Anfrage für eine Person dieser Art durchgeführt wird (Siehe Execs und Anpassungen (see page 47)).

Feld	Beschreibung
EXEC	Dieser Prozess wird ausgeführt, sobald eine Anfrage über die Daten einer Person durchgeführt wird. Beispielsweise wenn eine Person angelegt/gelöscht wird oder ihre Daten geändert werden.
EXEC für Personenänderungen	Dieser Prozess überschreibt den Prozess der bei einer Personenänderung für Services durchgeführt wird (siehe Services).
EXEC für Service-Requests	Dieser Prozess überschreibt den Prozess der bei der Serviceprovisionierung/Dekomissionierung aller Services für eine Person dieser Art durchgeführt wird.
EXEC für Passwortänderungen	Dieser Prozess wird ausgeführt wenn eine Anfrage zur Passwortänderung einer Person durchgeführt wird.

Berechtigungen

Mit folgenden Einstellungen steuern Sie welche Berechtigungen notwendig sind um Anfragen für Personen dieser Art zu stellen oder um entsprechende Informationen anzuzeigen.

Feld	Beschreibung
Neuanlage	Folgende Berechtigung wird benötigt um eine Person dieser Art anlegen zu können. Personen dieser Art erscheinen dann für Sie im Menü *Personen > Person anlegen*
Bearbeitung	Diese Berechtigung wird benötigt um die Daten einer Person zu bearbeiten.
Service anfragen	Diese Berechtigung wird benötigt um Services für eine Person anfordern oder löschen zu können.
Service anzeigen	Diese Berechtigung erlaubt es einem Benutzer die aktuellen Servicezuordnungen einer Person einsehen zu können.

Gruppen anfragen	Benutzer mit dieser Berechtigung können Änderungen der Active Directory Gruppenmitgliedschaften einer Person beantragen.
Gruppen anzeigen	Diese Berechtigung erlaubt es einem Benutzer die aktuellen Mitgliedschaften in Active Directory Gruppen einer Person anzuzeigen.
Verzeichnisse anfragen	Mit dieser Berechtigung kann gesteuert werden welche Personen Änderungen von Ordnerberechtungen für Personen dieser Art anfragen können.
Verzeichnisse anzeigen	Folgende Berechtigung erlaubt es einem Benutzer die aktuellen Verzeichnisberechtigungen einer Person anzusehen.

Verzeichnis- und Gruppenberechtigungen

Die Berechtigungen für Verzeichnisse und Active Directory Gruppen beziehen sich nur auf die Seite zur Bearbeitung von Personen. Für die Seite der Freigabenberechtigungen Active Directory Gruppen sind andere Berechtigungen vorgesehen.

LDAP Attribute

Feld	Beschreibung	Beispielwert
AD-Container	Hier kann ein Active Directory Container eingetragen werden, in welchen Personen dieser Art gespeichert werden. Wenden Sie sich an Ihren Betreuer um tenfold entsprechend für Ihre Umgebung einzurichten.	OU=External,OU=USR,OU=CERTEX,OU=AT

Einstellungen

Feld	Beschreibung
Niederlassungstypen	Hier kann man auswählen, welche Typen von Niederlassungen für eine Person dieser Art zulässig sind. Für Personen dieser Art lassen sich daraufhin Niederlassungen auswählen, welche von einer ausgewählten Art sind (siehe Unternehmen & Niederlassungen (see page 29)).
Auswählbare Personenarten	Hier können Sie festlegen welche Personenarten zulässig sind, wenn man die Art einer Person ändern möchte. Sollte hier keine Auswahl getroffen worden sein, so bleibt unabhängig der Konfiguration für das Feld *PERSON_TYPE*, das entsprechende Eingabefeld gesperrt. Stellen Sie auch sicher, dass sich die aktuelle Personenart selbst in der Auswahl befindet, wenn Sie diese Einstellung nutzen.

> ⚠ **Niederlassungstypen**
>
> In der aktuellen Version von tenfold existiert kein Wartungsschirm für die Niederlassungstypen. Diese müssen manuell in der Datenbank gewartet werden. Kontaktieren Sie hierfür bitte Ihren Betreuer.

Allgemeine Optionen

Feld	Beschreibung
Mehrere Niederlassungen	Ist diese Einstellung aktiviert, kann einer Person mehr als nur eine Niederlassung angezeigt werden. Auf der Seite der Personenänderungen wird daraufhin ein Mehrfachliste angezeigt, anstatt einer Dropdown-Auswahl
Ablaufdatum zwingend	Mit dieser Einstellung können Sie steuern ob für eine Person
Personenänderungen erlauben	Ist diese Einstellung deaktiviert, lässt sich eine Person dieser Art unbhängig der Eingestellten Berechtigungen nicht von Benutzern bearbeiten.
Personenbilder erlauben	Diese Einstellung aktiviert das Bearbeiten von Bildern bei Personen dieser Art. Wenn Sie diese Einstellung aktivieren, sollten Sie auch den Job *Active Directory Picture Sync* aktivieren, damit die bereits bestehenden Bilder aus dem Active Directory übernommen werden (siehe Jobs (see page 18)).
Tabs sperren	Ist diese Einstellung aktiviert, so werden bei der Anlage von Personen dieser Art die einzelnen Tabs für Services, Gruppen und Verzeichnisse erst freigeschalten wenn man den jeweiligen vorhergehenden Tab bearbeitet hat. Damit entsteht ein Workflow welcher ähnlich dem von üblichen Assistenten ist.
Ticketnummer anzeigen	Ist diese Einstellung aktiviert, kann man beim Speichern einer Person eine Ticketnummer angeben, welche in der daraus resultierenden Anfrage hinterlegt wird. Dies können Sie benutzen, wenn Sie ein Ticketsystem verwenden und die Ticketnummern in tenfold per Hand vergeben wollen, statt die Ticketnummer von Ihrem System generieren zu lassen.
Kommentar anzeigen	Mit der Aktivierung dieser Option wird beim Speichern eines Benutzers die Eingabe eines Kommentars für die Anfrage angezeigt. Dieser Kommentar wird dann in der daraus resultierenden Anfrage hinterlegt.
Zukünfitge Änderungen erlauben	Wenn Sie diese Option aktivieren, können Sie beim Speichern einer Person ein Datum hinterlegen. Die jeweilige Änderung wird dann für die Zukunft als Geplant markiert und erst an dem ausgewählten Datum durchgeführt. Die Anfrage muss im Vorfeld dennoch wie üblich genehmigt werden.

Personenanlage

Feld	Beschreibung
Namenscheck anzeigen	Mit aktivieren dieser Einstellung wird vor der Neuanlage einer Person überprüft ob eine Person mit diesem oder ähnlichem Vor/Nachnamen in tenfold bereits existiert. Damit kann vermieden werden, dass unterschiedliche Benutzer versuchen die gleiche Person anlegen wollen.
Benutzernamensvorschlag anzeigen	Mit dieser Einstellung werden vor der Personenanlage ein oder mehrere Benutzernamen generiert von denen der Benutzer einen auswählen kann. Auch kann er dann einen eigenen Benutzernamen eingeben und überprüfen ob dieser noch verfügbar ist.
Leeren User anlegen	Dies blendet bei der Personenanlage die Option *Leeren Benutzer anlegen* ein. Ein leerer Benutzer hat keine Services, Gruppen oder Verzeichnisse voreingestellt. Diese können aber im Laufe der Benutzeranlage händisch hinzugefügt werden.
Nach Vorlage anlegen	Dies blendet bei der Personenanlage die Option *Nach Vorlage anlegen* ein. Mit dieser Option kann ein Profil ausgewählt werden und sämtliche Services und Gruppen welche in dem Profil enthalten sind, werden der anzulegenden Person bereits hinzugefügt. Weitere Services und Gruppen können manuell hinzugefügt werden.
Nach vorhandener Person anlegen	Dies blendet bei der Personenanlage die Option *Nach vorhandener Person anlegen* ein. Hier kann eine bestehende Person aus tenfold ausgewählt werden und sämtliche Services und Gruppen, welche die Person besitzt werden der neu anzulegenden Person bereits hinzugefügt. Diese können manuell um weitere Services und Gruppen erweitert werden.
Passwort vergeben	Wird diese Option aktiviert, wird nach dem Speichern einer neuen Person nach einem Passwort gefragt, welches für diese Person eingerichtet wird, anstelle eines zufällig generierten Passwortes.

Tab: Genehmigungsworkflows

In diesem Tab können die Genehmigungsworkflows eingestellt werden, welche für Personen dieser Art gelten. Sollte kein Workflow eingerichtet worden sein, werden Anfragen zur Anlage/Löschung einer Person oder dem Ändern ihrer Daten sofort durchgeführt.

Um einen Workflow hinzuzufügen klicken Sie auf den Button *Hinzufügen* und ändern anschließend die Einstellungen in der neuen erschienenen Zeile in der Tabelle unterhalb. Im Aktionsmenü einer Zeile können Sie mit der Aktion *Entfernen* eine bestehende Zeile wieder löschen.

Folgende Einstellungen können in einer Zeile getroffen werden:

Feld	Beschreibung
Request-Quelle	Hier kann eingeschränkt werden für welche Quellen von Requests ein Genehmigungsworkflow gelten soll.
Request-Modus	Hier kann eingeschränkt werden ob der Workflow für Personenänderungen oder Passwortänderungen gültig sein soll.
Request-Typ	Hier kann eingeschränkt werden für welche Typen von Requests der Workflow angewendet werden soll.
Genehmigungsworkflow	Hier wird der Genehmigungsworkflow ausgewählt, welcher für die ausgewählten Filter gültig sein soll.

Wenn ein Request ausgelöst wird, so wird immer der Genehmigungsworkflow ausgewählt, dessen Einschränkungen am genauesten zu dem Request passen. Bevorzugt werden dabei Workflows bei welchen mehr Filter zutreffen als bei anderen. Sollten bei mehreren Workflows gleich viele Filter zutreffen, so haben die Filtereinstellungen in den Spalten von links nach rechts Vorrang. Das bedeutet, dass zum Beispiel die Request-Quelle Vorrang vor dem Request-Modus hat.

2.4.2 Personenlisten

Menü > Personen > Stammdaten > Personenlisten > Personenlisten verwalten

Hier lassen sich Listen von Personen erstellen, welche sich auf keine andere Art eingliedern lassen. Man könnte hier zum Beispiel Blacklists von Personen anlegen, welche bei einem Personenimport ignoriert werden sollen. Benutzer werden hierbei manuell in den Listen eingetragen.

Folgende Einstellungen lassen sich für eine Personenliste treffen.

Feld	Beschreibung	Beispielwert
Name	Der Name der Personenliste, welche in tenfold angezeigt wird.	SAP-Blacklist
Beschreibung	Eine informative Beschreibung der Liste, zum Beispiel um ihren Zweck festzuhalten.	

Mitglieder verwalten

Menü > Personen > Stammdaten > Personenlisten > [Name der Liste]

Nachdem Sie eine Personenliste erstellt haben, können Sie Mitglieder hinzufügen. Geben Sie dazu einfach die entsprechenden Daten an und klicken auf den Knopf *Hinzufügen.* Über den Befehl *Löschen* im Aktionsmenü eines Eintrages lassen sich entsprechende Einträge wieder aus der Liste entfernen.

Bearbeiten von Einträgen

Die Daten einer Zeile lassen sich nicht verändern sobald sie hinzugefügt worden sind. Möchten Sie eine Zeile bearbeiten, so löschen Sie sie und fügen sie danach erneut ein.

Folgende Einstellungen lassen sich zu einem Mitgliedseintrag treffen:

Feld	Beschreibung	Beispielwert
Person	Eine bestehende Person in tenfold	Max Mustermann (mmusterm)
Vorname	Der Vorname einer Person.	Max
Nachname	Der Nachname einer Person.	Mustermann
Personalnummer	Die Personalnummer einer Person.	4711
Benutzername	Der Benutzername einer Person.	mmusterm
Kommentar	Eine informative Beschreibung warum der Benutzer in der Liste ist	

Zusätzlich zu bestehenden Personen in tenfold lassen sich auch einfach nur Vornamen, Nachnamen, etc angeben falls Sie zum Beispiel eine Blacklist mit Benutzernamen anlegen wollen, welche Sie aus Fremdsystemen nicht übernehmen wollen.

2.4.3 Positionen

Menü > Personen > Stammdaten > Positionen

Bei Positionen handelt es sich um Rollen welche eine Person in Ihrer Organisation übernehmen können. Mit Positionen lassen sich Personen zum Beispiel in Angestellte und Führungspositionen einteilen. Eine andere Einteilung nach Tätigkeitsfeldern innerhalb einer Abteilung ist jedoch auch denkbar. Positionen dienen zum einen dazu, ihre Daten konsistent zu halten und zum anderen lässt sich über die Position einer Person eine automatische Profilzuordnung einrichten (Siehe Profile).

JOB_TITLE vs POSITION

Sowohl das Personenfeld JOB_TITLE als auch POSITION werden überlicherweise als Position bezeichnet. Beide beschreiben einen ähnlichen Datenbestand. Der Unterschied ist, dass es sich bei JOB_TITLE um ein Freitextfeld handelt und bei POSITION um eine Auswahlliste von vorgegebenen Einträgen. Weiters kann das Feld JOB_TITLE nicht zur automatischen Zuordnung von Profilen herangezogen werden.

Feld	Beschreibung	Beispielwert
Name	Der Name der Postion. Dieser Wert wird in tenfold angezeigt und kann in Anpassungen zum Beispiel auch in das Active Directory übertragen werden.	Angestellter, Abteilungsleiter, Betriebsrat, Geschäftsführung
EID	Eine ID welche in Fremdsystemen verwendet werden kann um die Position zu identifizieren.	123, P-17
Code	Ein Kürzel welches verwendet werden kann um zum Beispiel in das Active Directory geschrieben zu werden, wenn es nicht erwünscht ist den voll ausgeschriebenen Namen zu verwenden	DeptHead
AD-Container	Ein Container der angegeben werden kann falls es gewünscht ist Personen nach deren Position in das Active Directory einzugliedern. Bitte wenden Sie sich an Ihren Betreuer falls Sie dieses Feature nutzen möchten.	OU=Dept.Heads,OU=USR,OU=CERTEX,OU=AT
Parameter	Hier können Benutzerdefinierte Parameter hinzugefügt werden, welche in Anpassungen herangezogen werden können.	

2.4.4 Titel

Menü > Personen > Stammdaten > Titel

Hier lassen sich die Titel bearbeiten welche einer Person über die Personenfelder *PERSON_TITLE*, *POST_NAME_TITLE* und *PRE_NAME_TITLE* zugewiesen werden können (siehe Personenfelder). Dies dient hauptsächlich dazu Ihre Daten einheitlich zu halten und Doppel- bzw. Fehleingaben zu vermeiden.

Feld	Beschreibung	Beispielwert
Name	Der Name des Titels. Dieser wird in tenfold Angezeigt.	Herr, Frau, Dr., Ba, Bsc
EID	Eine externe ID welche zur Identifizierung eines Titels in Fremdsystemen verwendet werden kann.	M, W, title-1, DR, BSC
Code	Ein Kürzel für einen Titel, welcher verwendet werden kann, falls es nicht erwünscht ist de ausgeschriebenen Namen des Titels in das Active Directory zu schreiben	Hr., Fr.

Anrede	Gibt an ob der Titel als Anrede (Personenfeld *PERSON_TITLE*) dienen soll. Nur Titel die diese Schalftfläche aktiviert haben werden im Dropdown dieses Feldes angezeigt.	/
Vor Name	Gibt an ob es sich bei dem Titel um einen, üblicherweise Akademischen Titel, handelt welcher vor dem Namen geführt wird, wie zum Beispiel Dr. oder Mag. Nur Titel welche diese Option gewählt haben erscheinen in der Auswahl des Personenfeldes *PRE_NAME_TITLE*.	/
Nach Name	Gibt an ob es sich bei dem Titel um einen, üblicherweise Akademischen Titel, handelt welcher nach dem Namen geführt wird, wie zum Beispiel MSc oder BSc. Nur Titel welche diese Option gewählt haben erscheinen in der Auswahl des Personenfeldes *POST_NAME_TITLE*	/

2.5 Systemeinstellungen

2.5.1 Allgemeines zu Systemeinstellungen

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

Standardeinstellungen

Diese sind im Auslieferungszustand des Systems bereits vorhanden. Es kann lediglich der Wert angepasst werden, der Name ist fix.

Benutzerdefinierte Einstellungen

Es ist möglich neue Einstellungen zum System hinzuzufügen. Diese dienen primär dazu, um das Verhalten von selbst entwickelten EXECs (Funktionsbausteinen) steuern zu können. Es können sowohl der Name als auch der Wert angepasst werden. Eine Systemeinstellung kann als Paramter direkt in einen EXEC injiziert werden.

> **Passworte**
>
> Achtung: Die Systemeinstellungen eignen sich nicht dazu, die Zugangsdaten (Verbindung, Benutzer, Passwort und ähnliches) für eine Zielapplikation zu hinterlegen. Die Systemeinstellungen werden in der Datenbank nicht verschlüsselt gespeichert. Wenn Sie

Benutzer und/oder Passworte hinterlegen wollen, nutzen Sie stattdessen die Funktion zum Hinterlegen von Zugangsdaten (Menü > System > Zugangsdaten).

2.5.2 Verwaltung von Systemeinstellungen

Alle Systemeinstellungen anzeigen

Die Liste der Systemeinstellungen kann unter Menü > System > Systemeinstellungen angezeigt werden.

Neue Systemeinstellung anlegen

Mit dem Hinzufügen-Button kann ein neuer, benutzerdefinierter Eintrag angelegt werden.

Bearbeiten von Systemeinstellungen

Um eine bestehende Systemeinstellung zu bearbeiten, muss im Kontextmenü der betreffenden Eintrags die Aktion "Bearbeiten" gewählt werden.

Löschen von Systemeinstellungen

Es können nur benutzerdefinierte Systemeinstellungen gelöscht werden. Dazu muss im Kontextmenü der betreffenden Eintrags die Aktion "Löschen" gewählt werden.

2.5.3 Liste der Standardeinstellungen

Die nachfolgende Liste beschreibt die Standardeinstellungen, welche mit tenfold mitgeliefert werden. Der Hinweis "Experteneinstellung" deutet an, dass diese Einstellung nur von qualifizierten Systembetreuern mit entsprechendem Know-How angepasst werden sollten. Bei Fehlkonfiguration ist das System gegebenenfalls nicht mehr funktionsfähig. Auch Datenverlust kann nicht augeschlossen werden.

Name	Experten	Beschreibung
AccessManagement.defaultContextName	✓	Steuert die Bezeichnung für den Default-Kontext bei der Verwaltung von Applikationsberechtigungen. Rollen können in tenfold abhängig von einem Kontext (z.B. einem Mandaten) innerhalb einer Zielapplikation vergeben werden. Auch wenn eine Anwendung dies nicht unterstützt, muss zumindest ein Kontext verfügbar sein, auf welchem die Zuordnung der Rollen erfolgt. Dieser wird bei Bedarf von tenfold automatisch angelegt. Die Einstellung steuert die Bezeichnung die dieser Kontext erhalten soll.
Ads.defaultApprovePrivilege		Definiert die Berechtigung, welche zum Genehmigen von Requests für Gruppenänderungen notwendig ist, sofern bei der Gruppe kein Dateneigentümer definiert ist.
Birt.log.level	✓	Legt das Log-Level für die Reporting-Engine fest. Standardmäßig steht diese auf "ERROR", das heißt es werden nur schwerwiegende Fehler protokolliert. Wenn Probleme im Reporting auftreten, ist es sinnvoll diese Einstellung auf "DEBUG" zu setzen, um mehr Informationen zu erhalten.
Birt.repository	✓	Definiert den Pfad zu den Report-Vorlagen. Diese Einstellung sollte im Betrieb nicht geändert werden.
Exec.appServerLog	✓	Legt fest, ob im Logfile des Applikationsserver jeder EXEC, der durchgeführt wird, als Source-Code gelogt werden soll.
Exec.defaultEventSource	✓	Im Ereignisprotokoll in tenfold gibt es für jeden Eintrag eine Quelle. Diese beschreibt, wer den Eintrag protokolliert hat (ein EXEC, ein bestimmter Connector, etc.). Diese Einstellung legt die Bezeichnung für die Standardquelle fest, welche für alle Einträge gilt, die direkt in einem EXEC protokolliert werden.
ExecPlan.serviceRequest.codeFooter	✓	Legt den Source-Code fest, der (live während der Ausführung) in jeden EXEC nach der letzten Zeile eingefügt wird. Üblicherweise muss hier kein Wert festgelegt werden.

ExecPlan.serviceRequest.codeHeader	✓	Legt den Source-Code fest, der (live während der Ausführung) vor jedem EXEC eingefügt wird. Diese Einstellung eignet sich dazu, allgemein Befehle, wie beispielweise allgemeingültige "import"-Statements festzulegen.
Expenses.fiscalYearEnd		Diese Einstellung ist nur für den Bereich "Finanzen" relevant und legt das Datum des Geschäftsjahreswechsels fest.
Feature.dm		Mit dieser Einstellung wird festgelegt, ob die Funktionen Gruppenverwaltung und Fileserver aktiviert sein sollen. Wenn diese Einstellung auf N gestellt wird, so werden bestimmte Einträge im Menü "Windows" nicht mehr angezeigt. Darüber hinaus werden bestimmte Tabs in der Schnellsuche nicht angezeigt und bestimmte Tabs ("Gruppen" und "Verzeichnisse") sind auf der Maske "Person bearbeiten" nicht mehr verfügbar.
Feature.fm		Steuert, ob die Funktion "Finanzen" aktiviert ist. Wenn diese Einstellung deaktiviert wird (Wert = N), dann wird das Menü "Finanzen" ausgeblendet. Außerdem finden sich in den Beschreibungen und in der Funnktion "Services kaufen" keine Preisinformationen mehr.
JMS.queue.exchangeScan.name	✓	Legt den internen Warteschlangenname für Exchange-Scans fest.
JMS.queue.ntfsScan.name	✓	Legt den internen Warteschlangenname für Fileserver-Scans fest.
JMS.queue.sharepointScan.name	✓	Legt den internen Warteschlangenname für SharePoint-Scans fest.
JMS.server.url	✓	Legt den Namen des Warteschlangenservers fest. Wenn kein Wert angegeben wurde, wird der aktuelle Server (Applikationsserver) festgelegt. Diese Einstellung darf bis auf weiteres nicht geändert werden.
Job.recommendationMode		
LandingPage.news.text		Bestimmt den Text, welcher auf der Startseite unter dem Punkt "Neuigkeiten" angezeigt wird.
License.licenseFile		Es wird der Pfad zur Lizenzdatei festgelegt. Wenn diese EInstellung unsachgemäß angepasst wird, so lässt sich der Applikationsserver nicht mehr starten.

License.pubringFile		Es wird der Pfad zur Lizenzprüfdatei festgelegt. Wenn diese EInstellung unsachgemäß angepasst wird, so lässt sich der Applikationsserver nicht mehr starten.
List.search.rowsPerPage		Legt fest, wieviele Zeilen standardmäßig in Suchresultaten angezeigt werden
List.serviceRequest.daysBack		Legt fest, wieviele Tage in der Vergangenheit der Suchfilter auf der Maske "Requests" standardmäßig gestellt werden soll
Mail.default.from		Die Einstellung legt fest, welche Adresse als From: Adresse bei E-Mails verwendet wird, sollte der EXEC bei der Nutzung des E-Mail-Connectors nichts abweichendes definieren.
System.adminRole		Legt fest, welche Rolle die Rolle des Systemadministrators ist.
System.exec.updatePath		Definiert von welchem Pfad Updates für Standard-EXECs geladen werden. Diese Einstellung wird während einem Systemupgrade benötigt.
System.msia.updatePath		Legt fest, wo sich die Update-Packages für den tenfold Agent befinden. Diese werden über die automatisch Aktualisierung vom Applikationsserver verteilt.
System.setupMode		Diese Einstellung steuert ein systeminternes Verhalten. Sie muss immer auf N stehen.
System.url		Legt die URL des aktuellen Systems fest. Diese Einstellung wird häufig für Verlinkungen in E-Mails genutzt. Es sollte eine URL eingestellt werden, unter welcher den tenfold Applikationsserver von überall in der Organisation erreichbar ist.
System.personId		Legt die ID des Systembenutzers fest. Diese Einstellung sollte im Betrieb nicht angepasst werden.
System.sendEmails		Steuert, ob das System tatsächlich E-Mails versendet oder nicht. Die Einstellung kann auf N gestellt werden, was dazu führt, dass das System E-Mails zwar erstellt und protokolliert, aber nicht tatsächlich versendet. Diese Einstellung ist hilfreich, wenn man auf einem Testsystem bestimmte Abläufe testen möchte, ohne tatsächlich E-Mails an die betroffenen Personen zu versenden. Diese Einstellung ist für Testsysteme zu empfehlen.

System.showIds		Legt fest, ob auf der Oberfläche für Objekte auch die interne ID angezeigt werden soll. Diese Einstellung ist für Testsysteme zu empfehlen.
System.SingleSignOn		Steuert, ob SSO via Active Directory auf dem System aktiviert ist.
UI.dropDown.costCenter.order		Legt fest, ob bei der Auswahlbox für Kostenstellen zuerst der Code (Einstellung = 2) oder der Name (Einstellung = 1) angezeigt werden soll.
UI.help.visible		Diese EInstellung legt fest, ob auf den Masken in tenfold der Hilfe-Button für die Online-Hilfe zur Verfügung steht.
UI.home.createTicket.visible		Steuert, ob die Funktion "Ticket anlegen" auf der Startseite zur Verfügung stehen soll. Damit ist es möglich in Kombination mit einer entsprechenden Anbindung Tickets in tenfold zu erfassen und direkt in der Helpdesk-Lösung anzulegen.
UI.html.title		Legt fest, welcher Text in der Titelleiste des Browser angezeigt werden soll
UI.logo		Definiert den Pfad zum Logo, welches sich links oben im Menü befindet. Hier kann ein unternehmenseigenes Logo verwendet werden. Dieses sollte für optimale Darstellung die Abmesssungen 80x28 pixel aufweisen.
UI.newsPosition		
UI.personSearch.show*		Es existieren für dieses Muster zahlreiche Einstellungen. Diese legen fest, welche Spalten im Suchresultat für Personen angezeigt werden sollen. Diese Einstellung gilt für die Personensuche und die Schnellsuche.
UI.quicksearch.searchCostCenter		Legt fest, ob der Tab "Kostenstelle" in der Schnellsuche angezeigt werden soll.
UI.quicksearch.searchDepartment		Legt fest, ob der Tab "Abteilung" in der Schnellsuche angezeigt werden soll.
UI.quicksearch.searchOffice		Legt fest, ob der Tab "Niederlassung" in der Schnellsuche angezeigt werden soll.
UI.quicksearch.searchOu		Legt fest, ob der Tab "Organisationseinheit" in der Schnellsuche angezeigt werden soll.

3 Anpassungen

tenfold kann in vielerlei Hinsicht an Ihre Bedürfnisse angepasst werden. Die Anpassung von tenfold erfolgt durch EXECs, wobei es sich um Groovy(http://www.grovy-lang.org) Skripte handelt, welche in der tenfold-Datenbank gespeichert werden. Diese Skripte lassen sich durch Jobs (siehe Jobs (see page 18)) in gezielten Intervallen starten, oder werden im Laufe von verschiedenen Prozessen aufgerufen.

Bedeutung von Feldern

In tenfold lassen sich vielerlei Einstellungen zu Ihrer Organisation oder IT-Landschaft treffen. Manche Einstellungen sind relevant für die Standardkonfiguration, manche haben in der Grundeinstellung jedoch nur informativen Charakter, lassen sich jedoch in Anpassungen heranziehen. Felder welche Auswirkungen auf das Verhalten von tenfold haben, entweder in der Bedienung oder in Prozessen welche in der Standardkonfiguration enthalten sind, werden im folgenden mit 💡 markiert, solche die dies nicht tun mit 💡.

Eigene Anpassungen

Bitte nehmen Sie zur Kenntnis das nicht garantiert werden kann, dass Anpassungen die Sie selbst an tenfold vornehmen, mit zukünftigen Versionen von tenfold kompatibel sind.

4 Active Directory und Fileserver

Nachdem das System auf dem gewählten Server installiert wurde, gehen Sie folgendermaßen vor, um das System mit Active Directory® und Ihren Fileservern zu verbinden:

1. Einrichten einer Windows Domain (see page 48)
2. Einrichten des tenfold Agent (see page 54)
3. Einbinden von Freigaben (see page 66)

4.1 Einrichten einer Windows Domain

4.1.1 Einführung

Zu Beginn müssen die Einstellungen für jede Windows Domain hinterlegt werden, welche in tenfold integriert werden soll.

Multi-Domain-Umgebungen

tenfold ist grundsätzlich Multi- Domain-fähig. Für die Einrichtung mehrerer Domains ist jedoch tenfold Enterprise erforderlich. Wenn Sie nicht über die Enterprise Editon verfügen, können Sie keine neue Domain hinzufügen. In diesem Fall müssen Sie die Standard-Domain zur Einrichtung heranziehen.

4.1.2 Anlegen der Domain

Um eine neue Domain anzulegen, wählen Sie im tenfold Menü "Windows > Domänen" und klick Sie auf das (Hinzufügen) Icon im rechten oberen Bildschirmbereich.

Sie können eine bestehende Domain bearbeiten, indem Sie im Kontextmenü der gewünschten Domain die Option "Bearbeiten" wählen.

Ändern von Domains

Wenn Sie eine Domain eingerichtet haben, und die Domain initial mit tenfold synchronisiert haben (über den Abgleich der Benutzer oder anderen Objekte) dürfen Sie die Domain-Einstellungen nicht auf die Daten einer anderen Domain in Ihrer Umgebung ändern, da dies zu Inkonsistenzen führt.

Basiseinstellungen

Zuerst müssen die Basiseinstellungen der Domain festgelegt werden:

Parameter auf Maske	Beschreibung	Beispiel
Name	Hier wird der NETBIOS Name der Domain eingetragen	TENFOLD
Interaktion	Diese Einstellung kann in Funktionsbausteinen (EXECs) verwendet werden, um bestimmte Aktionen auf den jeweiligen Domains nicht auszuführen. ⚠ Diese Einstellung hat in der tenfold Essentials und Essentials Plus Edition keine Auswirkung.	
UPN Suffix	Hier wird der UPN (User Principal Name) Suffix der Domain hinterlegt.	tenfold.local
Agent	Diese Einstellung definiert welcher Agent für das Hinzufügen von Gruppenmitgliedschaften aus fremden Domains verwendet wird. Diese Einstellung ist nur in Multi-Domain-Umgebungen zu setzen.	

LDAP Verbindungseinstellungen

tenfold greift über LDAP auf das Active Directory zu. Die Zugangsdaten für die Verbindung zur Domain müssen im Karteireiter "LDAP Verbindungseinstellungen" hinterlegt werden:

Parameter auf Maske	Beschreibung	Beispiel
Host	Der FQDN des Domain-Controller, den tenfold für seine Verbindung nutzen soll. 💡 Sie können das Server-Icon neben dem Eingabefeld nutzen, um tenfold nach verfügbaren Domain-Controllern suchen zu lassen. Es öffnet sich ein Dialog mit allen gefundenen Servern. Um einen der Server zu übernehmen wählen sie "Auswählen" im Kontextmenü des gewünschten Servers.	srv01.tenfold.local
Authentifikation	Diese Einstellung steuert den Verbindungsmodus den tenfold für die LDAP Verbindung zu Active Directory nutzt	
Benutzername	Der vollqualifizierte Benutzernamen des Dienstkontos für die LDAP-Verbindung	svc-tenfold@tenfold.local

Passwort	Das Passwort des Dienstkontos Das Passwort wird verschlüsselt in der tenfold Datenbank gespeichert und ist für Datenbankbenutzer, die Zugriff auf die tenfold-Datenbank haben nicht lesbar	
Bestätigung	Zur Bestätigung muss das Passwort nochmals eingegeben werden	
LDAP-Version	Version des LDAP-Protokolls. Aktuell wird nur die Einstellung "2" unterstützt.	2
LDAP-Port	Der LDAP-Port für unsichere Verbindungen. Die Standardeinstellung ist 389. Wenn Ihr Active Directory für einen anderen Port konfiguriert wurde, so müssen Sie hier den entsprechenden Wert hinterlegen.	389
LDAPS-Port	Der LDAP-Port für verschlüsselte Verbindungen. Die Standardeinstellung ist 636. Wenn Ihr Active Directory für einen anderen Port konfiguriert wurde, so müssen Sie hier den entsprechenden Wert hinterlegen.	636
Zertifikatsvalidierung	Diese Einstellung steuert, ob tenfold bei einer sicheren LDAPS-Verbindung prüft, ob das vom Server bereitgestellte SSL-Zertifikat eine gültige Signatur besitzt. Wenn das Server-Zertifikat nicht von einer vertrauenswürdigen Stelle signiert wurde, so muss diese Einstellung deaktiviert werden.	J / N
SSL erzwingen	Diese Einstellung steuert ob alle LDAP-Verbindungen automatisch über eine verschlüsselte Verbindung gemacht werden sollen.	J / N

Testen der Verbindungseinstellungen

Die getroffenen Verbindungseinstellungen können ganz einfach über tenfold getestet werden. Dazu muss das Server-Icon im rechten oberen Bildschirmbereich geklickt werden. tenfold übernimmt die

jeweils in den Eingabefeldern getroffenen Einstellungen, auch wenn die Daten noch nicht über das Sichern-Icon gespeichert wurden. W

Organisationseinheit-Konfiguration

Um die Struktur des Active Directory in tenfold zu hinterlegen, müssen einige Einstellungen im Karteireiter "Organisationseinheit-Konfiguration" getroffen werden:

Konfiguration der Organisationseinheiten

Sie können jede Einstellung auf dieser Maske entweder durch Texteingabe einstellen, oder Sie nutzen jeweils das neben dem Eingabefeld befindliche Such-Icon um den Active Directory Browser zu öffnen. Hier kann die Organisationseinheit per Mausklick ausgewählt werden.

Parameter auf Maske	Beschreibung
Root-OU	Legt den Wurzelknoten für die Verarbeitung im Active Directory fest. Der Wert wird üblicherweise auf den obersten Knoten im Active Directory festgelegt.
OU für Benutzer	Legt die OU für die Benutzerkonten fest. In dieser OU werden neue Benutzerkonten angelegt. Beim Abgleich mit Active Directory werden jedoch Benutzerkonten aus allen OUs berücksichtigt.
OU für Administratoren	Legt die OU für die Administratorkonten fest.
OU für Org.Grp.	Legt die OU für Organisatorische Gruppen fest. Diese Gruppen werden genutzt, um Benutzer nach organisatorischen Merkmalen (z.B. Abteilungen) zu gliedern. Diese Gruppen sind zu unterscheiden von Fileservergruppen, welche genutzt werden, um den Zugriff auf eine Ressource (beispielsweise einen Ordner oder eine Mailbox) zu steuern.
OU für FSP	Legt die OU für Foreign Security Principals fest. Diese Einstellung muss nur bei Multi-Domain-Umgebungen angegeben werden
OU für Funktionsbenutzer	Legt die OU für die Funktionsbenutzer (=Dienstkonten) fest.
OU für Identitäten	Legt die OU für Identitätskonten fest.

OU für Gelöschte (Benutzer)	Legt die OU für gelöschte Benutzer fest. Wenn ein Benutzer über tenfold gelöscht wird, so erfolgt keine automatisch Lösung im Active Directory. Stattdessen wird der Benutzer lediglich deaktiviert und in diese spezielle OU verschoben. ⚠ Es sollte darauf geachtet werden, dass die GPO-Verknüpfungen auf der ausgewählten OE für deaktivierte, später zu löschende Benutzer richtig gewählt werden.
OU für Fileservergruppen	Legt die OU für Fileservergruppen fest. In dieser OU legt tenfold alle automatisch erzeugten Fileservergruppen an. Eine Ressourcengruppe wird üblicherweise dann angelegt, wenn ein Zugriff auf eine Ressource hergestellt werden muss, für den noch keine Ressourcengruppe existiert.

Zusätzlich können bestimmte Container von der Verarbeitung ausgeschlossen werden. Es sind jeweils folgende Einstellungen zu treffen:

Parameter auf Maske	Beschreibung
Ausgeschlossener Container	Hier kann eine OE ausgewählt werden, welche von der Synchronisation mit Active Directory ausgeschlossen werden soll
Ausgeschlossen von	Mit dieser Einstellung kann detaillierter festgelegt werden, wo sich der Ausschluss auswirken soll: • Object & Personen Sync: Benutzer und Gruppen aus der OE werden generell nicht in tenfold angelegt. • Object Sync: Benutzer und Gruppen werden nicht als Active Directory Objekte nicht tenfold angelegt. • Personen Sync: Benutzer werden nicht als Personen in tenfold angelegt

⚠ **Containereinstellungen**

Die getroffenen Einstellungen für die Organisationseinheiten werden im Auslieferungszustand berücksichtigt. Es ist jedoch möglich, die Auswirkung dieser Einstellungen im Rahmen des Customizing über Funktionsbausteine (EXECs) anzupassen. Das kann dazu führen, dass die hier getroffenen Einstellungen keine direkten Auswirkungen auf das Systemverhalten haben.

Berechtigungen für das Active Directory

Auf dem Karteireiter "Active Directory" können Einstellungen für die Berechtigungen für das Active Directory getroffen werden. Die jeweilige Einstellung einer Berechtigung bedeutet, dass nur Benutzer,

welche über die ausgewählte Systemberechtigung (über Zuweisung einer Rolle) die angegeben Operation durchführen können. Folgende Operationen sind durch die Einstellung betroffen:

Parameter auf Maske	Operation	Erreichbar über
Gruppe bearbeiten	Erlaubt es, eine Active Directory Gruppe in der aktuellen Domain zu bearbeiten. Es können dabei die Grundeinstellungen der Gruppe wie Name und Besitzer bearbeitet werden. Die Möglichkeit zur Bearbeitung der Mitglieder erfolgt über eine gesonderte Einstellung.	Menü: Windows > Gruppen > Vorhandene Gruppe bearbeiten > Kontextmenü > Bearbeiten
Gruppe löschen	Erlaubt es, eine ganze Active Directory Gruppe zu löschen.	Menü: Windows > Gruppen > Vorhandene Gruppe bearbeiten > Kontextmenü > Löschen
Mitglieder bearbeiten	Erlaubt es, die Mitglieder einer Active Directory Gruppen zu bearbeiten.	Menü: Windows > Gruppen > Vorhandene Gruppe bearbeiten > Kontextmenü > Mitglieder bearbeiten

Ausführungszeitpunkt

Die Änderung der Daten erfolgt nicht umgehend, sondern ist davon abhängig, wie der Genehmigungsworkflow konfiguriert ist, und wer gegebenenfalls als Dateneigentümer der Gruppe hinterlegt ist. Es ist somit nicht ausreichend, die eingestellte Berechtigung zu besitzen, um tatsächlich eine Änderung im Active Directory zu bewirken. Die Berechtigung steuer lediglich, welche Personen das Recht haben sollen, einen entsprechenden Antrag (Request) zu erstellen. Der Request unterliegt dann gegebenenfalls einer entsprechenden Freigabe.

Fokus

Diese Einstellungen beziehen sich lediglich auf Organisationsgruppen, beziehungsweise Gruppen, welche nicht als Fileservergruppen gekennzeichnet wurden. Fileservergruppen sind spezielle Gruppen, welche rein zur Verwaltung des Zugriffs auf bestimmte Ressourcen (wie einem Ordner oder einer Mailbox) dienen. Diese Gruppen können über tenfold nicht explizit bearbeiten werden, sondern werden automatisiert im Hintergrund verwaltet, wenn sich der Zugriff auf die betreffende Ressource ändert, beispielsweise über einen Antrag auf Zuordnung von Verzeichnisberechtigungen.

4.2 Einrichten des tenfold Agent

4.2.1 Allgemeine Informationen

tenfold erlaubt die bequeme Verwaltung und Visualisierung von Berechtigungen auf den Fileservern einer Organisation. Um eine performante Visualisierung der Daten zu ermöglichen, werden alle Verzeichnisse und deren Berechtigungen (ACLs) über den tenfold Agent (MSIA) eingelesen und in der tenfold Datenbank hinterlegt. Alle Auswertungen beziehen sich anschließend auf die in der tenfold Datenbank gespeicherten Daten, da eine Live-Abfrage aus Performance-Gründen nicht realisierbar ist.

Der tenfold Agent (MSIA) übernimmt im Bereich der File Server grundsätzlich zwei Aufgaben:

- Auslesen der Berechtigungen auf einem Fileserver
- Setzen von Berechtigungen auf einem Verzeichnis

Um diese Aufgaben wahrnehmen zu können, muss der jeweilige Agent in tenfold eingebunden und einige Informationen zum Fileserver hinterlegt werden.

Aus Performancegründen sollte je LAN, in dem sich einzubindende Fileserver befinden, ein Agent installiert werden. Der Agent muss in jedem Fall nicht zwingend auf dem Fileserver selbst installiert werden, da der Zugriff auf die Freigaben über den UNC-Pfad erfolgt (beispielsweise \ \server01\share_a). Somit sind auch SAN/NAS Geräte, denen ein NTFS-Dateisystem zugrundeliegt (oder die zumindest ein NTFS-Dateisystem simulieren) und über CIFS/SMB erreichbar sind in tenfold einbindbar. Beispiele hierfür sind Systeme von EMC ® oder NetApp®.

4.2.2 Agent installieren

Der tenfold Agent muss zuerst auf einem geeigneten System installiert werden (zu den Systemvoraussetzungen für den tenfold Agent siehe auch: Installationsvorbereitung). Zur Installation des Agent wird ein Setup-Programm zur Verfügung gestellt, mit dem der Dienst eingerichtet werden kann. Um den Agent zu installieren, starten sie das Setup-Programm und folgenden Sie den Anweisungen des Install-Wizard.

Notwendige Berechtigungen

Der Agent muss mit einem bestimmten Dienstkonto ausgeführt werden, welches bei der Installation festgelegt wird. Beachten Sie, dass dieses Dienstkonto über ausreichende Berechtigungen verfügen muss, um auf dem Fileserver Berechtigungen auszulesen und setzen zu können. Andernfalls ist die Nutzung nur eingeschränkt möglich. Eine andere Möglichkeit bieten die Optionen " backupRead" und "backupWrite", welche unterhalb detaillierter beschrieben werden.

4.2.3 Konfiguration des Agent

Der tenfold Agent verfügt über eine lokale XML-Konfigurationsdatei, welche die Konfiguration für diesen jeweiligen Agent steuert. Wenn für die Authentifizierung/Verschlüsselung zwischen Applikationsserver und Agent TLS gewählt wurde, müssen in der Konfigurationsdatei ein Benutzername und ein Passwort hinterlegt werden. Die Datei ist dementsprechend gegen unberechtigten Zugriff zu schützen.

Basiseinstellungen

Im Abschnitt "appSettings" der Datei können einige Basiseinstellungen vorgenommen werden. Wenn der Parameter nicht angegeben wurde, so gilt der jeweilige Default-Wert.

Einstellung	Beschreibung	Default-Wert	Beispiel
preserveInheritance	ℹ Diese Einstellung ist obsolet und wird von tenfold ignoriert.		true / false
ClientSettingsProvider .ServiceUri	ℹ Diese Einstellung ist obsolet und wird von tenfold ignoriert.		
authUser	Die Einstellung legt den TLS-Benutzernamen für die Authentifizierung zwischen tenfold Applikationsserver und tenfold Agent fest	leer	user
authPassword	Diese Einstellung legt das TLS-Passwort für die Authentifizierung zwischen tenfold Applikationsserver und tenfold Agent fest	leer	password
backupRead	Diese Einstellung legt fest, ob der Agent das Auslesen der Berechtigungen im sogenannten Backup-Operator-Mode durchführt. Es werden in diesem Fall beim Zugriff keine Berechtigungsprüfungen durch Windows durchgeführt. ⚠ Um diese Einstellung verwenden zu können, muss das Dienstkonto mit dem der tenfold Agent ausgeführt wird über die Berechtigung "Sicherungs-Operatoren" verfügen.	false	true / false

backupWrite	Diese Einstellung legt fest, ob der Agent beim Schreiben von Berechtigungen im sogenannten Backup-Operator-Mode durchführt. Es werden in diesem Fall beim Zugriff keine Berechtigungsprüfungen durch Windows durchgeführt. ⚠ Um diese Einstellung verwenden zu können, muss das Dienstkonto mit dem der tenfold Agent ausgeführt wird über die Berechtigung "Sicherungs-Operatoren" verfügen.	false	true / false
scanSharepointFiles	Legt fest, ob für SharePoint einzelne Dokumente eingescannt werden sollen oder ob einzelne Dokumente beim Scan ausgelassen werden.	false	true / false
usePowershellScripts	Diese Einstellung legt das Verhalten beim Scan von Exchange-Mailboxen fest. 💡 Aus Performancegründen wird in großen Exchange-Umgebungen empfohlen, diesen Wert auf "true" zu setzen.	false	true / false
ewsPoolSize	Legt fest, wie viele EWS (Exchange® Web Services) Verbdindungen für Scan-Vorgänge gleichzeitig zur Verfügung stehen	100	1-500
powershellMinPoolSize	Legt fest, wie viele parallele PowerShell Verbindungen mindestens durch diesen Agent zur Verfügung gestellt werden sollen	15	1-100
powershellMaxPoolSize	Legt fest, wie viele parallele PowerShell Verbindungen maximal durch diesen Agent zur Verfügung gestellt werden sollen	25	1-100
powershellOutOfProcess	Legt fest, ob der Powershellaufruf des PowershellServices in einem neuen Prozess gestartet werden soll 💡 Ist der Wert auf "false" gesetzt, werden die Einstellungen "powershellMajorVersion" und "powershellMinorVersion" ignoriert	false	true / false

powershellMajorVersion	Legt die Hauptversion der erstellten Powershellinstanz des PowershellServices fest. Die festgelegte Version muss auf dem lokalen Rechner installiert sein ⚠️ Dieser Wert wird nur beachtet wenn der Wert hinter "powershellOutOfProcess" auf "true" gesetzt ist	3	3
powershellMinorVersion	Legt die Nebenversion der erstellen Powershellinstanz des PowershellServices fest. Die festgelegte Version muss auf dem lokalen Rechner installiert sein ⚠️ Dieser Wert wird nur beachtet wenn der Wert hinter "powershellOutOfProcess" auf "true" gesetzt ist	0	0
pathScanDurationDepth	Diese Einstellung legt fest bis zu welcher Ordnertiefe, Logausgaben über die Scandauer eines Ordners geschrieben werden. Der Wert 0 deaktiviert diese Funktion	0	0-100
stompClientSize	Diese Einstellung legt die Anzahl der Verbindungen zu tenfold fest. Diese Einstellung wird bei Scans von NTFS, Exchange und Sharepoint verwendet. 💡 Ist die zu scannende Umgebung sehr schnell, wie eine lokale SSD mit NTFS-Dateisystem, empfiehlt sich die Anzahl der Verbindungen zu erhöhen, damit mehrere Threads gleichzeitig Nachrichten an tenfold senden können	20	1-100

Kommunikationseinstellungen

Der tenfold Agent muss mit dem tenfold Applikationsserver kommunizieren. Dies geschieht über SOAP-Webservice für alle Anfragen vom Applikationsserver zum Agent und mit STOMP (für high performance queueing) für alle Antworten vom Agent für den Applikationsserver. Im tenfold Agent können Sie den Port festlegen, auf welchem der tenfold Agent auf Anfragen wartet. Die

Defaulfeinstellung ist TCP-Port 8000. Um diese Einstellung zu ändern muss die Konfigurationsdatei an allen relevanten Punkten angepasst werden:

- in allen <add baseAdress> Anweisungen nach dem "*:"
- in der <add scheme> Anweisung über den Parameter "port"

STOMP

Der Port für die STOMP-Konfiguration für die Antworten für tenfold muss auf Seite des Applikationsservers angepasst werden.

Funktionen

In der Konfiguration kann hinterlegt werden, welche der folgenden Funktionen der Agent zur Verfügung stellt:

- NTFSSecure: Funktionalität für Fileserver (Lesen/Schreiben von Ordnern und Berechtigungen)
- Powershell: Bereitstellung der Ausführung von PowerShell Skripts über diesen Agent
- LocalSystem: Funktion zum Auslesen von lokalen Benutzern und Gruppen auf diesem System
- Exchange: Funktionalität für Exchange (Lesen von Mailboxen, Ordnern und Berechtigungen)
- Sharepoint: Funktionalität für SharePoint (Lesen von Sites, Listen und Items und deren Berechtigungen)

Um eine Funktion zu deaktivieren, muss der jeweilige <service> Eintrag deaktiviert werden. Es bietet sich an, den Eintrag nicht zu löschen, sondern lediglich per Kommentar zu deaktivieren. In XML wird alles, was sich zwischen den Zeichenketten <!-- und --> befindet als Kommentar gewertet. Die folgenden Beispiele zeigen den Unterschied zwischen einer aktivierten und einer deaktivierten Funktion:

Aktivierter Eintrag

```
<service name="NTFSSecure" behaviorConfiguration="MSIA_Secure_Behavior">
<host>
<baseAddresses>
<add baseAddress="https://*:8000/MSIA/NTFSSecure"/ (see page 54)>
</baseAddresses>
</host>
<endpoint address="" binding="basicHttpBinding"
bindingConfiguration="basicBindingConfig" contract="MSIA.INTFSSecure"
name="ntfsBindingConfig" bindingNamespace="http://NTFS"/ (see page 54)>
<endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange"/>
</service>
```

Deaktivierter Eintrag

<!--

<service name="NTFSSecure" behaviorConfiguration="MSIA_Secure_Behavior">
[... Inhalt wie oben ...]
</service>

-->

Was soll man aktivieren und was nicht?

Es sollten alle Funktionen, die nicht unmittelbar benötigt werden aus Sicherheitsgründen deaktiviert werden. Für die Einrichtung der Fileserver werden in jedem Fall die Funktionen "NTFSSecure" und "LocalSystem" benötigt. In Multi-Domain-Umgebungen ist zusätzlich die Funktion "Powershell" zwingend erforderlich

Wenn Sie in der Konfiguration Änderungen vorgenommen haben, müssen Sie den tenfold Agent neu starten.

Starten / Stoppen

Um den Agent zu starten, wechseln Sie in die Windows-Dienstverwaltung (Systemsteuerung > Verwaltung > Dienste) und suchen Sie den Eintrag "ISM MSIA".

- Klicken Sie mit der rechten Maustaste auf den Eintrag und wählen Sie "Start", um den Dienst zu starten.
- Um den Dienst wieder zu stoppen, klicken Sie erneut auf den Eintrag und wählen die Option "Stoppen"
- Alternativ wählen Sie Option "Neu starten" um den Agent in einem Durchgang zu stoppen und zu starten.

4.2.4 Agent in tenfold einbinden

Damit tenfold mit dem Agent kommunizieren kann, muss er in tenfold bekannt sein. Für die Einrichtung führen Sie folgende Schritte durch:

1. Wählen Sie Menü > Windows > Agents an
2. Klicken Sie auf das Hinzufügen Icon
3. Legen Sie einen Namen für den Agent fest (dieser dient lediglich zur Darstellung auf der tenfold Oberfläche)
4. Geben Sie die URL an, unter der der Agent erreichbar ist (z.B. http://srv99.tenfold.local:8000[1] - beachten Sie bitte das http:// als Prefix und geben Sie die korrekte Portnummer an)

[1] http://localhost:8000

5. Testen Sie, ob die Verbindung erfolgreich ist, in dem Sie das Aktualisieren-Icon im rechten oberen Bildschirmbereich klicken
6. Wenn die Verbindung erfolgreich ist, wird Ihnen der Computername, der Benutzername und die eingesetzte Agent-Version angezeigt

4.2.5 Agent über tenfold aktualisieren

Sobald der Agent lokal auf einem Server installiert wurde, kann er zentral über tenfold auf eine neue Version aktualisert werden. Dazu wählen Sie im Kontextmenü den Punkt "Version aktualisieren" und folgen den Anweisungen auf dem Dialog.

4.3 Berechtigungsgruppen

4.3.1 Allgemeines

Benötigte Berechtigung

Um die Konfiguration der Berechtigungsgruppen vorzunehmen, ist die Systemberechtigung "Resource Group Configuration Administration" (8091) erforderlich.

Werden mit tenfold Berechtigungen auf Fileserver / Verzeichnisse gesetzt, so werden diese Berechtigungen ausschließlich nach den Best Practices von Microsoft gesetzt. Das bedeutet, dass je Verzeichnis und Berechtigungsstufe entsprechende Gruppenstrukturen angelegt werden (welche genau, hängt von der Konfiguration ab). Für eine allgemeine Beschreibung der Best Practices (AGDLP-Prinzip) siehe AGDLP bei Wikipedia[2]. Um die Konfiguration festzulegen, wechseln Sie im Menü zu Windows > Fileservergruppen. Es können eine oder mehrere Konfigurationen hinterlegt werden, welche dann in den konfigurierten Windows Domains verwendet werden können. Eine Konfiguration kann in mehreren Domains verwendet werden und jeder Domain ist genau eine Konfiguration zugeordnet.

Scope

Die Konfiguration steuert den strukturellen Aufbau der Gruppen sowie die Namenskonvention. Die Organisationseinheiten, in denen die Gruppen abgelegt werden, wird jedoch bei den Einstellungen zur Domain konfiguriert (Einrichten einer Windows Domain (see page 48)).

[2] https://en.wikipedia.org/wiki/AGDLP

4.3.2 Anlegen einer neuen Konfiguration

Um eine neue Konfiguration anzulegen, klicken Sie auf die Schaltfläche "Hinzufügen" und nehmen Sie anschließend die nachstehende Einstellungen vor.

Namenskonvention

Die Namenskonvention innerhalb einer Konfiguration gibt an, wie Gruppen, die von tenfold zur Berechtigungsvergabe angelegt werden, benannt werden sollen. Es ist dabei möglich den Namen aus mehreren Bestandteilen zusammenzusetzen. Die Einstellung erfolgt im rechten Bereich in der Liste "Bestandteile". Die Reihenfolge kann dabei über die Schaltflächen "Aufwärts" und Abwärts" frei gewählt werden.

Folgende Bestandteile stehen zur Verfügung, welche zum Teil direkt auf der Maske zu konfigurieren sind:

- Präfix: Das Präfix wird je Konfiguration festgelegt. Das gewünschte Präfix wird in das Textfeld "Präfix" eingegeben.
- Server: Repräsentiert den bei der betroffenen Freigabe, auf dem sich das Verzeichnis befindet hinterlegte Feld "Servername"
- Freigabe: Repräsentiert den bei der betroffenen Freigabe, auf dem sich das Verzeichnis befindet hinterlegte Feld "Freigabename"
- Verzeichnis: Repräsentiert den gesamten Pfadnamen des betroffenen Verzeichnisses ab der Freigabe; Unterverzeichnisse werden dabei durch das gewählte Trennzeichen getrennt (z.B. Folder1\Folder2\Folder3 mit Trennzeichen "Unterstrich" wird zu Folder1_Folder2_Folder3)
- Gruppenbereich: Repräsentiert die Bezeichnung des jeweiligen Gruppentyps (global, lokal, universal). Die gewünschten Bezeichnungen (Abkürzungen) werden in den Textfeldern "Bez. lokale Gruppe", "Bez. globale Gruppe" und "Bez. universale Gruppe" festgelegt.
- Suffix: Es handelt sich hierbei um das Suffix der jeweiligen Berechtigungsstufe (Lesen & Ausführen, Ändern, etc.), für welche die Gruppe angelegt wird. Das Suffix für die jeweilige Berechtigungsstufe kann auf der Maske "Berechtigungssätze" geändert werden.

Strukturkonfiguration

Die wesentliche Einstellung zur Struktur der Gruppen wird über den RBAC-Modus festgelegt. Der RBAC-Modus definiert, welcher Gruppentyp oder Gruppentypen bei der Berechtigungsvergabe angelegt werden. Es stehen hierbei folgende Optionen zur Verfügung, welche anschließend kurz erklärt werden.

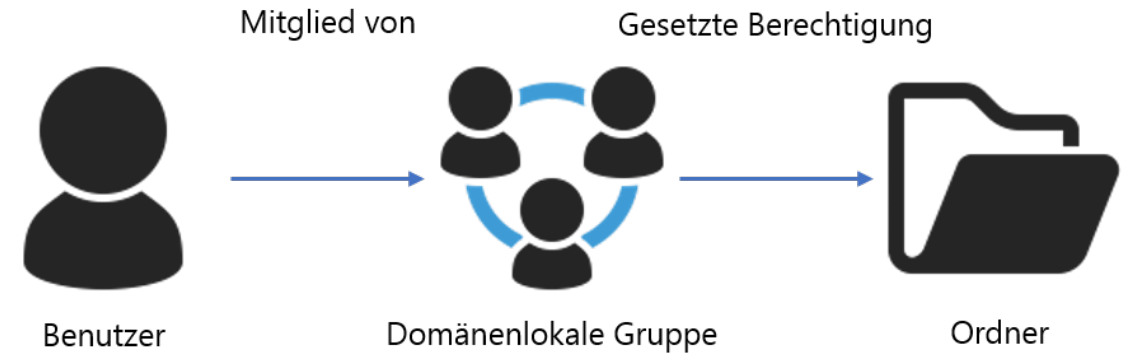
> **Single- vs. Multi-Domain**
>
> Nicht alle RBAC-Modi sind für jede Umgebung geeignet:

> Der Modus "AGGP/AGP" kann nur in Single-Domain Umgebungen genutzt werden. Der Modus "AGDLP - Benutzer in globaler Gruppe" sollte nur in Multi-Domain-Umgebungen verwendet werden.

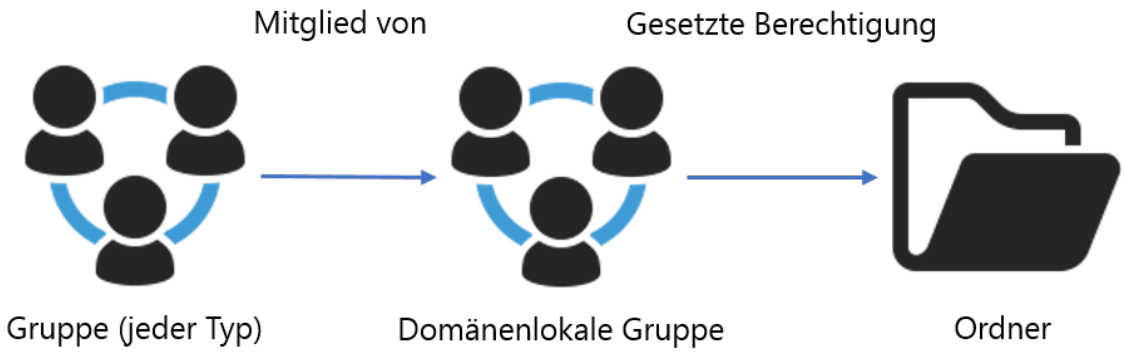
AGDLP - Benutzer in domänenlokaler Gruppe

- Es wird eine domänenlokale Gruppe als Berechtigungsgruppe in der Domain des Fileservers angelegt. Diese Gruppe wird in die ACL des Dateisystems eingetragen.
- Berechtigte Benutzer aus jeglichen Domains werden als direkte Mitglieder der Berechtigunsggruppe aufgenommen
- Berechtigte Gruppen jeglichen Typs aus jeglicher Domain werden als direkte Mitglieder der Berechtigungsgruppe aufgenommen

Für berechtigte Benutzer sieht der Aufbau folgendermaßen aus:



Für berechtigte Gruppen sieht der Aufbau folgendermaßen aus:



AGDLP - Benutzer in globaler Gruppe

- Es wird eine domänenlokale Gruppe als Berechtigunsggruppe in der Domain des Fileservers angelegt. Diese Gruppe wird in die ACL des Dateisystems eingetragen.

Die restliche Verarbeitung hängt davon ab, ob das zu berechtigende Objekt ein Benutzer oder eine Gruppe ist.

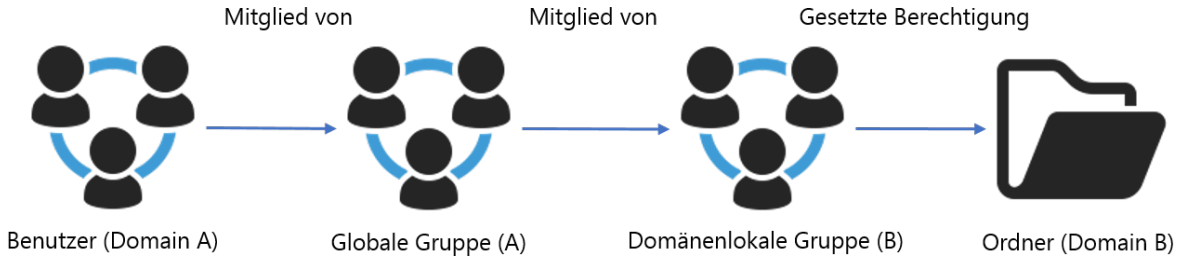
Für Benutzer:

- Es wird eine globale Gruppe in der Domain des berechtigten Benutzers angelegt
- Diese Gruppe wird als Mitglied der domänenlokalen Fileservergruppe aufgenommen.
- Berechtigte Benutzer werden als direkte Mitglieder der globalen Gruppe in ihrer eigenen Domain aufgenommen.

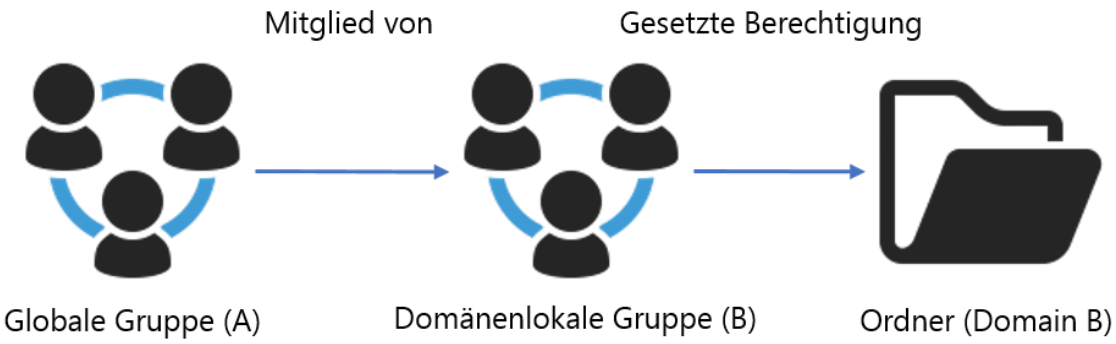
Für Gruppen:

- Die zu berechtigende Gruppe wird direkt als Mitglied der domänenlokalen Fileservergruppe aufgenommen
- Achtung: Es wird keine separate globale Gruppe in der Domain der zu berechtigenden Gruppe angelegt

Für berechtigte Benutzer sieht der Aufbau folgendermaßen aus:



Für berechtigte Gruppen sieht der Aufbau folgendermaßen aus:



AGUP/AUP

- Es wird eine universale Gruppe als Berechtigungsgruppe in der Domain des Fileservers angelegt. Diese Gruppe wird in die ACL des Dateisystems eingetragen.
- Berechtigte Benutzer aus jeglichen Domains werden als direkte Mitglieder der Berechtigunsggruppe aufgenommen
- Berechtigte Gruppen jeglichen Typs aus jeglicher Domain werden als direkte Mitglieder der Berechtigunsggruppe aufgenommen

Aufbau

Der Aufbau der Gruppen ist analog zum Modus "AGDLP - Benutzer in domänenlokaler Gruppe" - lediglich der Gruppentyp ändert sich auf "Universal".

AGGP/AGP

- Es wird eine globale Gruppe als Berechtigungsgruppe in der Domain des Fileservers angelegt. Diese Gruppe wird in die ACL des Dateisystems eingetragen.
- Berechtigte Benutzer werden als direkte Mitglieder der Berechtigunsggruppe aufgenommen (es können nur Benutzer aus der gleichen Domain berechtigt werden)
- Berechtigte Gruppen jeglichen Typs aus jeglicher Domain werden als direkte Mitglieder der Berechtigunsggruppe aufgenommen

Aufbau

Der Aufbau der Gruppen ist analog zum Modus "AGDLP - Benutzer in domänenlokaler Gruppe" - lediglich der Gruppentyp ändert sich auf "Global".

Multi-Domain

Dieser Modus ist nicht für Multi-Domain-Umgebungen geeignet, da Benutzer aus anderen Domains nicht Mitglied der globalen Berechtigungsgruppen werden können, welche auf dem Fileserver gesetzt wurden.

4.3.3 Konfiguration in einer Domäne verwenden

Einstellen der Konfiguration

Nachdem Sie die Konfiguration abgeschlossen haben, können Sie diese in den konfigurierten Domains verwenden:

- Öffnen Sie die Konfiguration für die jeweilige Domain und wechseln zum Karteireiter "Fileserver" (Einrichten einer Windows Domain (see page 48)).
- Wählen Sie unter dem Punkt "Fileservergruppen" die gewünschte Konfigurationseinstellung aus.

Änderungen

Achtung: Es ist absolut nicht empfohlen, diese Einstellung nachträglich zu ändern, sobald auf dem betroffenen Fileserver bereits Änderungen durch tenfold durchgeführt wurden, und somit entsprechende Gruppen angelegt wurden. Das System verhindert das Ändern der Einstellung nicht aktiv, eine Änderung darf allerdings nur nach entsprechender Prüfung und von Personen mit entsprechendem technischen Know-How erfolgen.

Konfiguration der Organisationseinheiten

Um die Konfiguration zu vervollständigen, muss noch festgelegt werden, in welchen Organisationseinheiten im Active Directory die von tenfold generierten Gruppen gespeichert werden sollen. Diese Konfiguration ist mehrstufig. Folgende Einstellungen können, abhängig vom gewählten RBAC-Modus, getroffen werden.

Domainweite Einstellung der OE für Berechtigungsgruppen von Fileservern aus der Domain

Im einfachsten Fall wird für eine gesamte Domain eine OE festgelegt, in welcher alle Berechtigungsgruppen abgelegt werden. Diese Einstellung wird am Karteireiter "Organisationseinheit-Konfiguration" im Feld "OU für Fileservergruppen" eingestellt. Diese Einstellung gilt grundsätzlich für die gesamte Domain.

Freigabespezifische Einstellung der OE für Berechtigungsgruppen der betreffenden Freigabe

Ist es nicht gewünscht, dass alle Gruppen in der gleichen OE abgelegt werden, so kann je Freigabe eine alternative OE definiert werden. Diese dient als Ablageort für alle Gruppen die für Verzeichnisse unter der betreffenden Freigabe angelegt werden. Um eine freigabespezifische Einstellung festzulegen, muss auf der Maske zur Konfiguration der Freigabe (siehe Einbinden von Freigaben (see page 66)) die Einstellung "Organisationseinheit für Fileservergruppen" von "Übernehmen" auf "Überschreiben" umgestellt werden. Anschließend kann die gewünschte, freigabespezifische OE im Textfeld "DN" festgelegt werden.

Spezielle Einstellungen für den Modus "AGDLP - Benutzer in globaler Gruppe"

Diese folgenden Einstellungen sind nur verfügbar, wenn der RBAC-Modus der für die Domain hinterlegte Konfiguration "AGDLP - Benutzer in globaler Gruppe" ist.

Multi-Domain

Diese Einstellung ist nur für Multi-Domain-Umgebungen sinnvoll.

In diesem Fall ist es möglich, nicht zur festzulegen, in welcher OE die domänenlokal Berechtigungsgruppen für die Fileserver aus dieser Domain abgelegt werden sollen. Es ist darüber hinaus möglich festzulegen, in welcher OE der anderen Domains die entsprechenden globalen

Gruppen angelegt werden sollen, in welche die Benutzer als Mitglieder aufgenommen werden. Es steht hierbei für jede Domain ein Karteireiter zur Verfügung, in der entweder die domainweite Einstellung der Domain übernommen werden kann (default), oder ob eine andere OE als Ablageort definiert werden soll.

4.3.4 Bearbeiten einer Konfiguration

Um eine bestehende Konfiguration zu bearbeiten, wechseln Sie im Menü zu Windows > Fileservergruppen. Anschließend wählen Sie in der Tabelle die entsprechende Konfiguration aus und wählen den Punkt "Bearbeiten" im Aktionsmenü.

Änderungen

Achtung: Es ist absolut nicht empfohlen, eine Konfiguration nachträglich zu ändern, sobald diese in einer Domain konfiguriert wurde, und auf einem der Fileserver der Domain Änderungen durch tenfold durchgeführt wurden, und somit entsprechende Gruppen angelegt wurden. Das System verhindert das Ändern der Einstellung nicht aktiv, eine Änderung darf allerdings nur nach entsprechender Prüfung und von Personen mit entsprechendem technischen Know-How erfolgen.

4.3.5 Löschen einer Konfiguration

Um eine bestehende Konfiguration zu löschen, wechseln Sie im Menü zu Windows > Fileservergruppen. Anschließend wählen Sie in der Tabelle die entsprechende Konfiguration aus und wählen den Punkt "Löschen" im Aktionsmenü.

Löschen von genutzten Konfigurationen

Eine Konfiguration kann nur gelöscht werden, wenn sie aktuell nicht in einer der konfigurierten Domains eingestellt ist. Versuchen Sie eine genutzte Konfiguration zu löschen, erhalten Sie eine entsprechende Warnmeldung. In diesem Fall müssen Sie die Einstellung bei allen Domains auf eine andere Konfiguration ändern. Anschließend können Sie die Konfiguration löschen. Beachten Sie jedoch unbedingt die Hinweise oberhalb betreffend Konfigurationsänderungen.

4.4 Einbinden von Freigaben

4.4.1 Auswahl der Domäne

Um einen Fileserver in tenfold einzubinden, müssen einige Einstellungen festgelegt werden. Um diese Einstellungen festzulegen, wählen Sie Menü > Windows > Domänen. Klicken Sie "Bearbeiten" im

Kontextmenü der Domäne in der sich der Fileserver befindet. Wählen Sie anschließend den Karteireiter "Freigaben" aus.

4.4.2 Einstellungen für die Domäne

Bestimmte Einstellungen können für die gesamte Domäne festlegt werden:

Einstellung	Beschreibung	Beispiel
Besitzer	Diese Einstellung legt fest, wer als Besitzer für Verzeichnisse eingetragen werden soll, welche über tenfold angelegt werden	TENFOLD \Administrator
Benutzer mit Vollzugriff	Über diese Einstellung kann festgelegt werden, dass für ein bestimmter Benutzer (oder eine bestimmte Gruppe) automatisch die Berechtigung "Vollzugriff" auf jedes über tenfold angelegte Verzeichnis erhält. Dies ist inbesondere wichtig, wenn ein Verzeichnis mit deaktivierter Vererbung angelegt wird. Wird hierbei durch tenfold kein Vollzugriffsbenutzer (oder Gruppe) festgelegt, so verliert tenfold jeglichen Zugriff auf dieses Verzeichnis. Es sollte für diese Einstellung eine Gruppe hinterlegt werden, in welcher das Dienstkonto des tenfold Agent Mitglied ist.	TENFOLD\fs-admins

4.4.3 Einstellungen für einen Fileserver

Um eine neue Freigabe auf einem Fileserver hinzuzufügen wählen Sie die Schaltfläche "Neue Freigabe" an. Sie können pro Domain beliebig viele Freigaben definieren.

Freigaben bearbeiten

Sie können die aktuellen Einstellungen zu einer Freigabe bearbeiten, indem Sie das Kontextmenü der jeweiligen Freigabe die Aktion "Bearbeiten" auswählen.

Es öffnet sich ein Dialog, auf welchem einige Einstellungen zu dieser Freigabe festgelegt werden müssen:

Einstellung	Beschreibung	Beispiel
Name	Diese Einstellung dient rein als Bezeichnung der Freigabe auf der tenfold Oberfläche.	Projektlaufwerk
Pfad	Der Pfad legt den UNC-Pfad fest, unter welchem die Freigabe für den jeweils hinterlegten Agent erreichbar ist	\\srv-fs01\projects
Agent	Wählen Sie hier den Agent aus, der für die Verarbeitung (Scan/Administration) der Freigabe verantwortlich ist. Aus Performancegründen sollten Sie einen Agent wählen, der sich im gleichen LAN wie der Server befindet	
Scan-Tiefe	Legt fest bis auf welche Hierarchiestufe der Agent den Fileserver scannen soll. Um die gesamte Freigabe zu scannen, geben Sie 99 als Wert an. Um die Performance zu steigern kann hier ein geringer Wert festgelegt werden. Dabei ist allerdings zu beachten, dass alle Verzeichnisse, die unter der gewählten Ebene liegen nicht im Reporting aufscheinen.	99
Bearbeitungstiefe	Legt fest, bis auf welcher Ebene durch tenfold Änderungen an der Freigabe durchgeführt werden dürfen. Um die Bearbeitung auf allen Ebenen zu ermöglichen, geben Sie als Wert 99 an. Mit dieser Einstellung können Sie verhindern, dass Benutzer beispielweise auf Verzeichnisse in der 5. Ebene neue Berechtigungen setzen können.	99
Sortiernummer	Diese Einstellung legt die Sortierreihenfolge der Freigaben auf den entsprechenden Masken fest. Sie können numerische Werte größer gleich 1 vergeben.	1
Aktiv	Dieses Kennzeichen legt fest, ob diese Freigabe angezeigt wird oder ob sie verborgen wird. Darüber hinaus werden inaktive Freigaben bei der Synchronisation mit dem Fileserver nicht berücksichtigt.	ja / nein

Planung erlaubt	Dieses Kennzeichen legt fest, ob Requests für diese Freigabe geplant werden können. Wenn diese Option aktiviert ist und Berechtigungen auf einem Ordner verändert werden, prüft das System, ob für die Änderung Operationen in den ACL des Fileserver notwendig sind. Wenn das der Fall ist, so wird der Request 1 Minute in die Zukunft geplant, um zu erreichen, dass die Verarbeitung im Hintergrund geschieht. ⚠ NTFS-Operationen können, besonders auf oberen Ordnerebenen viel Zeit in Anspruch nehmen (durch das Setzen der Vererbungen in den untergeordneten ACLs). Durch die Verarbeitung im Hintergrund, erhälter der Anwender sofort wieder die Kontrolle über tenfold und die Verarbeitung des Requests läuft im Hintergrund ab.	ja / nein
LST oberste Ebene	Legt fest, ob druch tenfold auch auf der der obersten Ebene eine LST-Gruppe (Listgruppe) angelegt werden soll.	ja / nein
Berechtigungen / Anzeige	Legt fest, welche Berechtigung für einen Benutzer erforderlich ist, damit die Ordnerstruktur und Berechtigungen auf der Freigabe angezeigt werden können. Es erfolgt hierbei keine weitere Einschränkung nach bestimmten Ordnern.	
Berechtigungen / Bearbeitung	Legt fest, welche Berechtigung für einen Benutzer erforderlich ist, damit die Ordnerstruktur und Berechtigungen auf der Freigabe bearbeitet werden können.	
Berechtigungen / Genehmigung	Diese Einstellung legt fest, welche Genehmigung erforderlich ist, um Requests für diese Freigabe genehmigen zu können.	
Dateneigentümer / Bearbeitung		

Lokale Gruppen / Computername	Wenn gewünscht ist, dass bei einem Windows File Server lokale Gruppen und Benutzerkonten berücksichtigt werden, so muss hier der NETBIOS-Computername des Servers eingetragen werden, von dem die lokalen Konten ausgelesen werden können (für diese Einstellung muss die Funktion "LocalSystem" beim jeweiligen Agent zwingend aktiviert sein). Wenn sich die jeweilige Freigabe auf einem Domain-Controller (Primär oder Sekundär) befindet, so darf diese Einstellung auf keinen Fall gesetzt werden, da Domain Controller keine lokalen Benutzer und Gruppen kennen und sich durch diese Einstellung Inkonsistenzen ergeben können.	SRV-FS01

4.4.4 Scan der Freigaben

Nachdem Sie die Freigabe konfiguriert haben, müssen Sie tenfold initial mit der Freigabe synchronisieren. Dazu muss der Job "Share Sync" ausgeführt werden.

Für eine Beschreibung wie dazu vorzugehen ist siehe: Jobs in tenfold (see page 18)

5 Connectoren

5.1 Connector: Microsoft Exchange

5.1.1 Einleitung

Dieses How-to zeigt die Konfiguration von Tenfold und Exchange 2013, um die Berechtigungsverwaltung zu nutzen.

5.1.2 Remote-Kommunikation zwischen MSIA und Exchange 2013/2010

Wird der MSIA nicht direkt auf dem Exchange Server installiert müssen einige Voraussetzungen erfüllt werden.

Im weiteren How-To wird der Pc, auf dem der MSIA installiert ist, als **Client** bezeichnet und der Exchange Server als **Server**.

Vorraussetzungen

- Exchange Management Shell muss auf dem **Client** installier sein
- System Management Framework 3(oder höher, je nach Windows Server Version) muss auf dem **Client** installiert sein - https://www.microsoft.com/en-us/download/details.aspx?id=34595
- Es wird ein Benutzer benötigt, Berechtiung **ApplicationImpersonation**

```
New-ManagementRoleAssignment -Role "ApplicationImpersonation" -User <username>
```

und der Rollengruppe **OrganizationManagement** auf dem **Server**

```
Add-RoleGroupMember "Organization Management" -Member <username>
```

-> Das ermöglicht die Kommunikation via Powershell und EWS

> Um Zugriff auf Öffentliche Ordner zu erhalten, muss der Benutzer ein Postfach besitzen.

> **Warnung**
>
> Es kann bis zu einem Tag dauern, dass die Berechtigungen seitens Exchange repliziert werden.

- Sicherstellen das der Benutzer am **Server** "Remote Powershell Enabled" ist.

```
Get-User <username> | fl RemotePowerShellEnabled
```

  Wenn *False* zurückgegeben wird, muss folgender Befehl durchgeführt werden

```
Set-User Administrator -RemotePowerShellEnabled $True
```

- MSIA auf **Client** installiert.

> Für Performance-Verbesserungen, bitte Exchange 2010 Performance Verbesserung lesen.

Credentials

- Wenn Credentials für EWS verwendet werden, darf nur der Benutzername angegeben werden (z.B. nur mmustermann statt tenfold\mmustermann oder mmustermann@tenfold.local).

> Im Moment wird nur die Eingabe eines Benutzeres unterstützt, welcher sich in der selben Domäne befindet wie Exchange Server.
> Falls ein Benutzer aus einer anderen Domäne verwendet werden soll, muss dieser direkt bei dem Service eingetragen werden, unter welchem MSIA lauft.

Related articles

Connector: Microsoft Exchange (see page 71)

Connector: PowerShell (see page 73)

Exchange 2010 Performance Verbesserung

Exchange: Anlegen einer Mailbox mit tenfold (see page 73)

5.2 Connector: PowerShell

5.2.1 Microsoft Exchange

Um Exchange Powershell Scripts wie beispielsweise "Enable-Mailbox" zu verwenden, muss der tenfold User bzw. der User mit welchem der MSIA betrieben wird in die Exchange Rolle „Organization Management role“ hinzugefügt werden.

Hierfür muss am Exchange Server mittels der „Exchange Management Shell“ folgenden Befehl ausgeführt werden:

```
New-ManagementRoleAssignment -Role "Organization Management role" -User <username>
```

Nach der Ausführung des Befehls ist der angegeben Benutzer berechtigt die jeweiligen Exchange Powershell Scripte auszuführen.

Zum Testen der Konfiguration kann der Enable-Mailbox Befehl folgendermaßen eingerichtet werden: Exchange: Anlegen einer Mailbox mit tenfold (see page 73)

5.2.2 Exchange: Anlegen einer Mailbox mit tenfold

Zum Anlegen einer Mailbox über tenfold müssen die folgenden Schritte durchgeführt werden:

Erstellen des Scripts in tenfold

Hierfür muss im Menüpunkt "Administration" -> "Scripts" ein neues Script erstellt werden, welches danach im jeweiligen EXEC verwendet werden muss.

```
Param([string]$username, [string]$database)

Set-ExecutionPolicy RemoteSigned

$session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri http://<Exchange-Server-
URL>/PowerShell
If ($session.state -ne 'Opened') {
    return 'Failed to create remote PowerShell session'
    exit
}

Import-PSSession $session

Enable-Mailbox -Identity $username -Alias $username -Database $database -DomainController
 <AdDomainControllerUrl>
```

```
Remove-PSSession $session
```

Erstellen des EXECs

Der folgende EXEC zeigt den Aufruf des oben angeführtem Scripts welcher unter dem Alias 'mailboxCreateScript' zur Verfügung steht.

```
// -----------------------------------------------
//  Request parameters
// -----------------------------------------------
def person = request.person
def pm = person.masterdata
def database = "<database_name>"

// -----------------------------------------------
//  Define script parameters
// -----------------------------------------------
def params = [:]
params["username"] = pm.userName
params["database"] = database

// -----------------------------------------------
//  Execute powershell script
// -----------------------------------------------
powershell.endpointUrl = msiaUrl.value
powershell.execute(mailboxCreateScript, params)

// -----------------------------------------------
//  Set request status to done
// -----------------------------------------------
request.status = RequestStatus.done
```

Connector: Microsoft Exchange (see page 71)

Connector: PowerShell (see page 73)

Exchange 2010 Performance Verbesserung

Exchange: Anlegen einer Mailbox mit tenfold (see page 73)

5.3 Connector: SAP

Dieses How-to zeigt die Konfiguration des tenfold SAP Connectors zur Verwaltung von Benutzerkonten und Berechtigungszuordnungen (es werden sowohl Profile als auch Rollen unterstützt).

5.3.1 Installation des SAP JCO Moduls

Zu Beginn muss das SAP JCO Modul im tenfold Applikationsserver installiert werden. Sollte der SAP JCO nicht bereits auf dem Serversystem eingerichtet sind, sind dazu folgende Schritte notwendig

1. Das Modul ".../agent/SapJcoConnector/jboss-module/sap-jco-module.zip" muss in den Installationspfad ".../ISM/jboss-as/modules/..." entpackt werden.

Anschließend muss das Modul in der standalone.xml des tenfold Applikationsservers eingetragen werden:

```
<subsystem xmlns="urn:jboss:domain:ee:1.0">
    <global-modules>
                ...
                <module name="at.certex.ism.connectors.sap" slot="main"/>
                ...
        </global-modules>
</subsystem>
```

Gegebenenfalls muss die entsprechende .dll Datei aus ".../at/certex/ism/connectors/sap/main/lib/..." zusätzlich nach C:\Windows\system32\ kopiert werden.

5.3.2 Freischaltung der BAPI

tenfold benötigt für die Benutzerverwaltung in SAP einen Dienstbenutzer, welcher über die Berechtigungen verfügt folgende BAPI via RFC aufzurufen:

- BAPI_USER_ACTGROUPS_ASSIGN
- BAPI_USER_ACTGROUPS_DELETE
- BAPI_USER_CHANGE
- BAPI_USER_CREATE1
- BAPI_USER_GET_DETAIL
- BAPI_USER_GETLIST
- BAPI_USER_LOCACTGROUPS_ASSIGN
- BAPI_USER_LOCACTGROUPS_READ
- BAPI_USER_LOCK
- BAPI_USER_UNLOCK

5.3.3 Verbindungseinstellungen

Um eine Verbindung mit dem SAP System herstellen zu können, müssen folgende Verbdindungsdaten vorhanden sein.

> **ZBV**
>
> im Falle eines ZBV-Verbunds bezieht sich dies auf das Zentralsystem der ZBV

- Mandant
- Benutzer (des Dienstbenutzers, welcher über die entsprechenden RFC-Berechtigungen verfügt)
- Passwort
- Sprache
- System (DNS oder IP)
- Systemnummer